UNIVERSIDAD CARLOS III DE MADRID
ESCUELA POLITÉCNICA SUPERIOR
Departamento de Ingeniería Mecánica

INGENIERÍA INDUSTRIAL

PROYECTO FIN DE CARRERA

ANÁLISIS RAMS

AUTOR: MARTA ZÁRATE FRAGA

TUTOR: Dr. JUAN CARLOS GARCÍA PRADA

FEBRERO, 2012

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. OBJETIVOS

El objetivo principal de este proyecto es la realización de una plantilla en *Microsoft Office Excel 2007*, para la realización de cualquier análisis RAMS. De esta forma se evitará que cada vez que se quiera realizar un análisis RAMS se tenga que empezar de cero. Esta aplicación es especialmente útil para analistas sin experiencia, reduciendo el tiempo de búsqueda de qué información es conveniente introducir en el análisis, qué información se ha de obtener y qué pasos hay que seguir.

La plantilla servirá como plantilla de partida, ya que, aunque todos los análisis deben tener unos inputs y outputs comunes, cada análisis tendrá unos datos distintos, ya que de cada sistema tendremos una cantidad de información distinta y se necesitará una información de salida distinta. El analista deberá ajustar la plantilla a sus necesidades.

El segundo objetivo del proyecto consiste en un informe en el que se explique en qué consiste el análisis RAMS, para qué sirve, paso a paso cómo se ha de realizar y qué resultados se obtienen.

La idea original del proyecto era realizar un análisis RAMS completo que sirviera como ejemplo para la realización de futuros proyectos, aportando un mayor entendimiento de los pasos a seguir en el análisis RAMS, pero fue imposible obtener suficientes datos reales sobre algún sistema. Y la invención de esto datos resultaba una tarea ardua y, a la vez, podía confundir a los analistas a la hora de utilizarlo como ayuda. Por lo que hemos tenido que utilizar como ejemplo ilustrativo: “Puertas automáticas de un vagón de una línea de metro con cierre de andenes” de “Creus Sole, Antonio (2005). *Fiabilidad y Seguridad*”.

2. INTRODUCCIÓN

El análisis RAMS, acrónimo de Reliability (fiabilidad), Availability (disponibilidad), Maintainability (mantenibilidad) y Security (seguridad), permite pronosticar para un período determinado de tiempo la disponibilidad y el factor de servicio de un proceso de producción, basado en su configuración, en la fiabilidad de sus componentes y en la filosofía de mantenimiento. En este estudio nos centraremos en el análisis de la fiabilidad, disponibilidad y mantenibilidad, aunque hablaremos indistintamente de análisis RAMS o análisis RAM.

La fiabilidad y la disponibilidad hacen referencia a la capacidad de un sistema para operar correctamente. Esta capacidad depende, entre otros, de los factores siguientes:

- Modos de fallo en la aplicación específica y el entorno.
- La probabilidad de que suceda cada fallo o, alternativamente, la tasa de fallo.
- El efecto de un fallo en la funcionalidad del sistema.

La mantenibilidad está inversamente relacionada con la duración y el esfuerzo requerido por las actividades de mantenimiento. Se centra en las medidas preventivas, para eliminar o disminuir las vulnerabilidades y amenazas en general. Tiene como objetivo evitar cualquier tipo de fallo mediante la detección de los primeros síntomas de anomalía. De esta manera, se toman las medidas adecuadas para anticipar la resolución a un problema inminente, evitando así las posteriores medidas correctivas y caídas o degradaciones del funcionamiento del sistema. Entre los factores que afectan la mantenibilidad se pueden destacar los siguientes:

- Tiempo de realización del mantenimiento.
- Tiempo para la detección, identificación y localización de fallos.
- Tiempo para restablecer un sistema en caso de fallo.
- Todos los modos de operación y mantenimiento requeridos durante todo el ciclo del sistema.

El objetivo de la seguridad de funcionamiento es proporcionar un producto que cumpla con las necesidades finales del usuario, a un bajo coste y en el tiempo límite prefijado. O bien, se considera la seguridad de funcionamiento como las características propias que le permite comportamientos funcionales especificados

(RAMS) en un tiempo determinado, con una duración establecida y sin daños a sí mismo o al ambiente.

Existen relaciones entre la Fiabilidad, la Disponibilidad, la Mantenibilidad y la Seguridad de funcionamiento. A mayor Seguridad, menor Disponibilidad y viceversa. Aumentando la Mantenibilidad y la Fiabilidad se consigue incrementar la Disponibilidad y la Seguridad de funcionamiento.

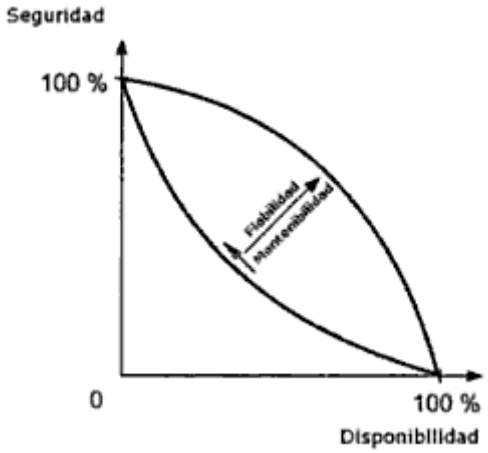

Figura 2.1: Relaciones Fiabilidad, Mantenibilidad, Disponibilidad y Seguridad

La base fundamental de este análisis es la selección de los MTTF(1), MTBF(2) y MTTR(3) que mejor caracterizan los diversos equipos del sistema de producción, tomados de bancos de datos genéricos de la industria, experiencia propia y opinión de expertos.

El análisis se sustenta en un modelo de simulación que toma en cuenta la configuración de los equipos, los fallos aleatorios, las reparaciones, las paradas parciales y totales y el mantenimiento planificado.

Durante la ejecución de un estudio RAMS, se realiza la adecuada caracterización probabilística de los procesos de deterioro que afectarán los equipos, sub-sistemas y sistemas asociados al citado proceso de producción a fin de pronosticar la mayoría de los escenarios de paros o fallos. Adicionalmente, se identifican acciones para minimizar la ocurrencia de estos escenarios y finalmente se identifican las implicaciones económicas de cada escenario, comparándolo con el escenario basado en “Las Mejores Prácticas” (Best Practices), a fin de contribuir con el establecimiento de estrategias óptimas de mantenimiento para el manejo del negocio.

(1) MTTF: Mean Time To Failure (Tiempo promedio para fallar)
(2) MTBF: Mean Time Between Failure (Tiempo promedio entre fallos)
(3) MTTR: Mean Time To Repare (Tiempo promedio para reparar)

3. DEFINICIÓN DE TASAS DE FALLO Y REPARABILIDAD

Algunos parámetros de medición usados comúnmente para estudiar los fallos que se presentan en un sistema determinado son los siguientes:

- **Tiempo promedio entre fallos (MTBF)** es para un período estable en la vida del componente o sistema, el valor medio de la duración de tiempo entre fallos consecutivos contados como la razón del tiempo observado y el número de fallos bajo condiciones estables. También utilizaremos el *Tiempo promedio para fallar* (MTTF), que, en rigor, únicamente es de aplicación para los componentes no reparables; no obstante, utilizaremos ambos conceptos de manera indistinta.

  El tiempo promedio entre fallos para datos exponencialmente distribuidos es:

$$MTTF \approx MTBF = \frac{1}{\lambda} \quad (3.1)$$

  siendo λ la *tasa de fallos* (fallos/hora).

- **Tiempo Promedio Para Reparar (MTTR)** es el tiempo promedio requerido para reparar un componente o un sistema. Para calcular este tiempo se usa la siguiente fórmula:

$$MTTR = \frac{1}{\mu} \quad (3.2)$$

  donde μ es la *Tasa de reparación* (reparaciones/hora)

4. FIABILIDAD

4.1 DEFINICIÓN DE FIABILIDAD

Se define como fiabilidad de un equipo la probabilidad de que dicho equipo se mantenga en funcionamiento correcto durante un tiempo determinado y bajo unas condiciones determinadas de marcha o actuación; en consecuencia, si estas condiciones cambian, la fiabilidad cambiará también, por lo que deberá extremarse la prudencia a la hora de comparar valores de fiabilidad de equipos idénticos que funcionen bajo condiciones distintas.

La fiabilidad, se representa por R(t). El valor complementario de R(t) se conoce como función acumulada de la probabilidad de fallo, se representa por F(t) y representa la probabilidad de que el equipo falle al cabo de un tiempo t.

$$R(t) = 1 - F(t) \qquad (4.1)$$

A partir de R(t) y de F(t) podemos definir una nueva función f(t) que se denomina función de densidad de la probabilidad de fallo:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \qquad (4.2)$$

De las *ecuaciones (4.2)* se deducen las siguientes:

$$R(t) = \int_t^{\infty} f(t)dt \qquad (4.3)$$

$$F(t) = \int_0^t f(t)dt \qquad (4.4)$$

La función f(t) representa la probabilidad de que un equipo que estaba en funcionamiento en el instante inicial t = 0 falle en el intervalo de tiempo (t, t + dt).

La relación entre f (t) y R(t) es otra nueva función, λ (t), conocida como tasa de fallo, la cual se define como la probabilidad de que un equipo que llega al instante t en perfecto funcionamiento falle en el intervalo (t, t + dt):

$$\lambda(t) = \frac{f(t)}{R(t)} \qquad (4.5)$$

Cuando la tasa de fallo es constante e independiente del tiempo; es decir, cuando:

$$\lambda(t) = constante = \lambda \qquad (4.6)$$

entonces:

$$MTTF = \frac{1}{\lambda} \qquad (4.7)$$

Si se conoce el número de fallos *n* que se han producido en un equipo durante un tiempo *t*, podemos estimar fácilmente el valor de MTTF mediante el cociente:

$$MTTF = \frac{t}{n} \qquad (4.8)$$

4.2 DEFINICIÓN DE FALLO Y TIPOS DE FALLO

Se define fallo, al cese de la capacidad de un elemento para realizar la función requerida. Los fallos pueden clasificarse de acuerdo con su criticidad o con su naturaleza.

El concepto de criticidad de un fallo está relacionado con la gravedad de las consecuencias que puede provocar. Si únicamente atendemos al impacto en el servicio, los fallos pueden clasificarse en significativos, importantes y menores, cuyas definiciones se recogen en la *Tabla 4.1*.

CATEGORÍA DE FALLO	DEFINICIÓN
SIGNIFICATIVO	Fallo que impide la prestación del servicio o que provoca un retraso en el servicio superior al periodo especificado.
IMPORTANTE	Fallo que debe ser corregido para que el equipo logre el rendimiento especificado pero que no provoca un retraso superior al especificado para el fallo significativo.
MENOR	Fallo que no impide que el equipo logre el rendimiento especificado y que no cumple con los criterios para ser considerado fallo significativo o importante.

Tabla 4.1: Categorías de fallos atendiendo a su impacto sobre la disponibilidad del servicio.

Si además de los daños en el propio equipo, se tienen en cuenta los daños producidos en las personas y en el medioambiente, los fallos pueden clasificarse en cuatro niveles, tal y como se muestra en la *Tabla 4.2*, siendo necesario establecer cuantitativamente qué se entiende por importante, apreciable y despreciable, a fin de reducir al máximo la subjetividad a la hora de calificar el fallo.

CATEGORÍA DE FALLO	FUNCIÓN	EQUIPO	AMBIENTE	PERSONAS
CATASTRÓFICO	Pérdida de una función esencial	Produce daños importantes		Puede causar muerte o daños corporales
CRÍTICO				Presenta riesgos despreciables de muerte o de daños personales
NO CRÍTICO	Funcionamiento degradado	No causa daños apreciables		No representa daños importantes
MENOR		Causa daños despreciables		No presenta riesgo de daños

Tabla 4.2: Niveles de gravedad de los fallos cuando se consideran los daños al equipo y su repercusión en las persona y en el medioambiente

De acuerdo con su naturaleza, los fallos pueden ser evidentes u ocultos al operador. Un fallo es evidente, cuando produce un efecto en el sistema. Por el contrario, un fallo se dice que es oculto cuando necesita de un evento posterior para ser detectado, lo que suele ser habitual en los sistemas de control o de detección y en los sistemas formados por dos equipos en los que uno está en activo y el otro está en reposo hasta que el anterior falle.

4.2.1 Causas de fallos

El concepto físico de fiabilidad, que expone que cualquier componente está definido por su resistencia R y suele soportar una carga C cuando está en funcionamiento, permite afirmar que los fallos pueden ser debidos a una resistencia inadecuada del componente, a una sobrecarga aplicada sobre el mismo o a ambas cosas a la vez.

Una resistencia inadecuada significa que el componente no es apto para realizar las funciones previstas, lo cual puede ser debido a un diseño deficiente, a un montaje defectuoso o a un mantenimiento inadecuado.

La sobrecarga puede producirse ocasionalmente o constantemente a lo largo del tiempo y puede tener un carácter intencionado o casual.

En ocasiones sucede que aunque la resistencia inicial sea la adecuada, las condiciones de trabajo a que se somete el componente producen una disminución progresiva de su resistencia a lo largo del tiempo hasta llegar a ser inferior a la carga

aplicada; es el caso de los materiales sometidos a fatiga, desgaste o corrosión por ejemplo. También puede suceder que la acción combinada de varias cargas distintas pueda provocar una debilitación de la resistencia del componente, por ejemplo, el fenómeno de fluencia que se produce en los materiales sometidos a altas temperaturas y esfuerzos de tracción.

4.3 VARIABILIDAD DE LA TASA DE FALLO

La constancia de la tasa de fallo indica que la aparición de los fallos es fruto del azar, que los fallos se presentan de forma aleatoria y por tanto, independientemente del tiempo de funcionamiento del equipo. Esto suele ser habitual para los componentes electrónicos pero no para la mayoría de los componentes industriales sometidos a fenómenos de desgaste, corrosión o fatiga, en los que la tasa de fallo aumenta con el tiempo de funcionamiento.

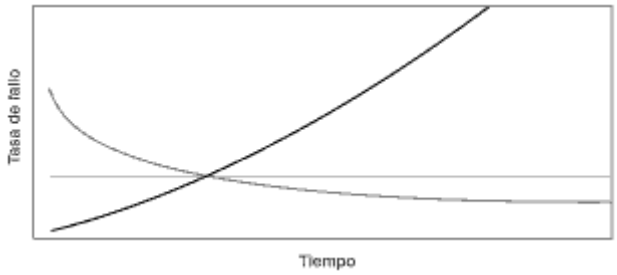

Figura 4.1: Formas de variación de la tasa de fallo con el tiempo.

En otras ocasiones, la tasa de fallo disminuye con el tiempo de funcionamiento del equipo; es el caso de aquellos componentes con una tensión inicial debida a una desalineación o un ajuste inadecuado producidos durante la fase de montaje, y que puede desaparecer a lo largo del tiempo por un proceso de acomodación del componente en su alojamiento. La *Figura 4.1* muestra los tres casos descritos de variación de la tasa de fallo con el tiempo.

En los equipos reparables, dada su complejidad, prima un comportamiento sin modo de fallo predominante, lo que da la apariencia de un modo de fallo aleatorio o de tasa de fallo constante; no obstante, para que ello sea así se requiere que las sucesivas reparaciones dejen el equipo tan bueno como nuevo. Si la reparación no ha sido la adecuada el equipo quedará peor que nuevo y en tal caso, la tasa de fallo aumentará. Por otra parte, el continuo desarrollo de la ingeniería puede permitir la situación del componente averiado por otro de mayor fiabilidad; en tales condiciones, la reparación dejará el equipo mejor que nuevo y por tanto, con una tasa de fallo menor.

En ocasiones, puede suceder que un mismo equipo adopte a lo largo del tiempo la tres configuraciones descritas anteriormente en la secuencia que aparece en la *Figura 4.2*, dando lugar a lo que se conoce por su forma como curva de la bañera y en la cual, el periodo de tasa decreciente se denomina de mortalidad infantil (al producirse en el periodo inicial de funcionamiento del equipo), mientras que el periodo de tasa creciente se denomina de envejecimiento (por producirse en el periodo final de funcionamiento del equipo); por su parte, el periodo central de tasa constante es el que determina la vida útil del equipo.

Durante muchos años se ha creído que la curva de la bañera era un patrón general de comportamiento; sin embargo, estudios realizados pusieron de manifiesto que solo un 4% de los componentes presentaba este comportamiento.

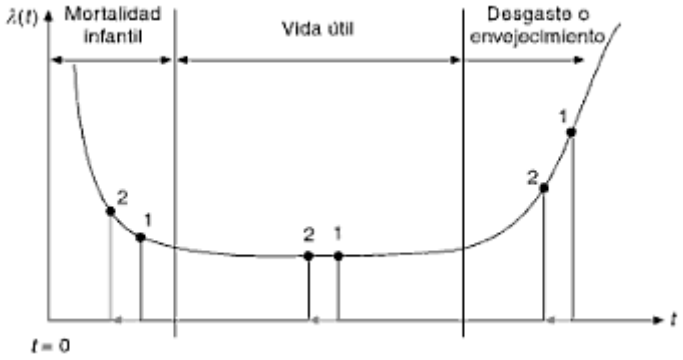

Figura 4.2: Curva de la bañera

4.4 FIABILIDAD DE LOS EQUIPOS COMPLEJOS

Cuando un equipo alcanza cierta complejidad se hace difícil determinar su fiabilidad, debiendo descomponerse en equipos más simples de los cuales se conozca su fiabilidad. El diagrama resultante de esta descomposición se conoce como diagrama de bloques de fiabilidad (RDB) y únicamente está formado por aquellos equipos que influyan en la fiabilidad global del equipo más complejo y en el que las conexiones entre tales equipos no tienen por qué ser físicas sino que pueden ser conexiones lógicas. Existen dos configuraciones básicas denominadas: sistema serie y sistema paralelo, las cuales estudiaremos a continuación.

Sistema serie: Su representación básica es la que se muestra en la *Figura 4.3*. En un sistema serie, la señal que se introduce en R_1 sólo podrá salir de R_S si todos los componentes intermedios son operativos.

Figura 4.3: Representación esquemática de un sistema serie.

Por tanto, la probabilidad de que un sistema serie esté en servicio exige que todos los componentes que lo forman lo estén también y por ello, deberá cumplirse que:

$$MTBF_S = \frac{1}{\lambda_S} = \frac{1}{\sum \lambda_i} \qquad (4.9)$$

De donde se demuestra que en un sistema serie, la fiabilidad del sistema es siempre inferior a la fiabilidad del componente menos fiable y además, dicha fiabilidad disminuye, al aumentar el número de componentes (*Figura 4.4*).

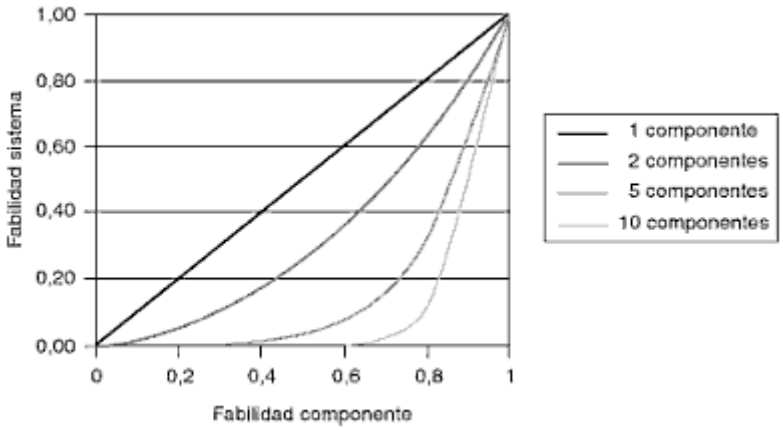

Figura 4.4: Variación de la fiabilidad del sistema serie en función de la fiabilidad de cada componente y del número de componentes del sistema.

Sistema paralelo: Se representa como se muestra en la *Figura 4.5*, por lo que una señal que se introduzca a la izquierda de la misma, para salir por la derecha bastará que haya al menos un componente operativo; es decir, el sistema fallará únicamente cuando todos los componentes hayan fallado simultáneamente.

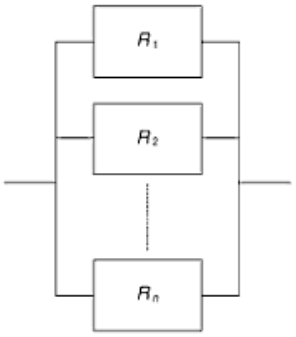

Figura 4.5: Representación esquemática de un sistema paralelo.

Por tanto: $MTBF_S > MTBF_i$ de cualquiera de los componentes del sistema.

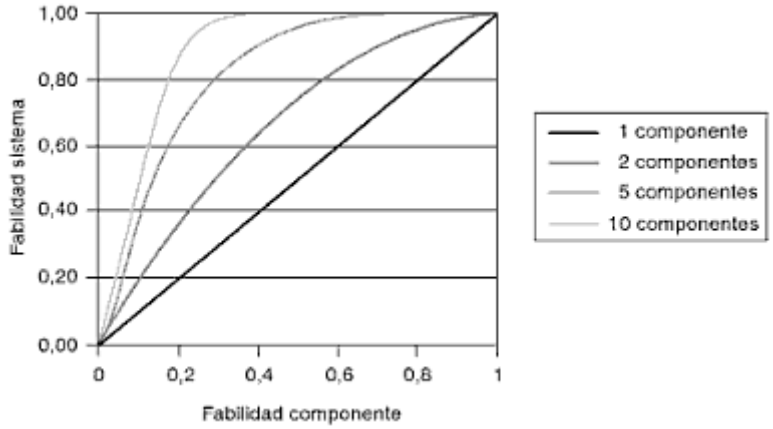

Figura 4.6: Variación de la fiabilidad de un sistema paralelo en función del número de componentes y de la fiabilidad de los mismos.

Cuando, como es habitual, los equipos que están en paralelo son todos iguales y en el caso de que la fiabilidad siga la ley exponencial, entonces el MTTF, del sistema puede calcularse fácilmente por la fórmula:

$$MTTF_S = \frac{1}{\lambda}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) \qquad (4.10)$$

Cuando el sistema funciona únicamente con uno o varios equipos simultáneamente y el resto se ponen en servicio solo si alguno de los equipos en funcionamiento falla, estamos ante lo que se denomina redundancia pasiva.

La fórmula que da el valor del MTTF para un sistema formado por N equipos operando y n equipos pasivos es la siguiente:

$$MTTF = \frac{1+n}{N\lambda} = \frac{1+n}{N} \cdot MTTF_i \quad (4.11)$$

La *ecuación (4.11)* considera que el sistema de conmutación es perfecto. La dificultad en caso contrario está en que el fallo del conmutador suele estar oculto y sólo será evidente cuando se solicite trabajar al equipo pasivo y no antes, lo que entraña ciertas dificultades.

5. MANTENIBILIDAD

5.1 DEFINICIÓN DE MANTENIBILIDAD

Cuando se produce un fallo en un equipo, se necesita un tiempo para detectar en qué componente se ha producido y para repararlo o sustituirlo por uno nuevo a fin de dejar el equipo en condiciones de funcionamiento. Se define como mantenibilidad, la probabilidad de que un equipo que ha tenido un fallo sea puesto de nuevo en funcionamiento, mediante la aplicación de ciertas acciones, dentro de un tiempo t que se conoce como tiempo de restauración. La mantenibilidad, por tanto, no está asociada únicamente a las características técnicas de la instalación sino también a las capacidades, experiencias y medios técnicos de los equipos de trabajo, por lo que los valores de mantenibilidad obtenidos con distintos equipos de trabajo pueden ser diferentes, al no ser iguales las capacidades y experiencias de sus miembros, como tampoco necesariamente las herramientas o útiles específicos empleados por cada uno de ellos.

La mantenibilidad se representa por M(t) y se expresa por la ecuación:

$$M(t) = \int_0^t g(t)dt \qquad (5.1)$$

en la que g(t) es la función densidad de probabilidad de los tiempos de restauración y representa la probabilidad de que un sistema averiado esté reparado en el instante t, sabiendo que se inició la acción de restauración en el instante t = 0.

Al igual que se estableció para la fiabilidad, llamaremos tasa de restauración a la probabilidad condicional de completar la acción de mantenimiento correctivo durante el intervalo de tiempo (t, t + dt), suponiendo que la acción comenzada en el instante t = 0 no se haya completado antes del tiempo t. Se representa por μ(t) y vale:

$$\mu(t) = \frac{g(t)}{1-M(t)} \quad (5.2)$$

De las ecuaciones anteriores se deduce que:

$$M(t) = 1 - e^{-\mu(t)\cdot t} \qquad (5.3)$$

Si se conoce la expresión matemática de la función g(t), podemos calcular la media de sus valores mediante la expresión:

$$m = \int_0^\infty t \cdot g(t)dt = MTTR \qquad (5.4)$$

que se conoce como tiempo medio de restauración y que suele emplearse como medida de la mantenibilidad del equipo.

Si la tasa de restauración μ(t) es constante:

$$MTTR = \frac{1}{\mu} \qquad (5.5)$$

En este caso, la mejor medida de la mantenibilidad de un equipo se obtiene mediante el cociente entre la suma de los tiempos de restauración t_r y el número total de fallos n; es decir:

$$MTTR = \frac{\sum_{r=1}^{R} t_r}{n} = \frac{t_g}{n} \qquad (5.6)$$

5.2 CLASES DE MANTENIMIENTO

Fundamentalmente, existen tres clases de mantenimiento: el correctivo, el preventivo y el de mejora.

El **mantenimiento correctivo** es el que se realiza cuando se ha producido el fallo en el equipo y comprende todas las actividades necesarias para restablecer su capacidad operativa inicial. Por su propia naturaleza, el mantenimiento correctivo es difícilmente programable (únicamente cuando los fallos son de escasa entidad) y dadas sus repercusiones, es una actividad indeseable que se pretende minimizar; como hemos visto anteriormente, la definición de mantenibilidad hace referencia fundamentalmente al mantenimiento correctivo.

El **mantenimiento preventivo** aparece en el momento que los costes provocados por los fallos (en general, pérdidas continuas de la producción) empiezan a ser importantes y también cuando aumenta el interés por los aspectos de la calidad y fiabilidad. Esta clase de mantenimiento apareció cuando se observó que la ejecución de ciertas operaciones más o menos sencillas, tales como la limpieza, la lubricación o las inspecciones, realizadas sistemáticamente cada cierto tiempo, retrasaba la aparición de los fallos y en ocasiones, incluso, llegaba a evitarlos. El mantenimiento preventivo mejora la fiabilidad del equipo y además tiene la ventaja de poderse programar, es decir, de ejecutar en el momento más favorable.

Las diferentes actividades de mantenimiento preventivo reciben el nombre genérico de revisiones. Cuando se realizan con una frecuencia inferior al año se denominan revisiones de ciclo corto, mientras que las revisiones que se realizan con una frecuencia superior al año se denominan revisiones de ciclo largo. Por su parte,

las revisiones que se realizan aproximadamente hacia la mitad de la vida del equipo suelen denominarse revisiones generales y se caracterizan por la sustitución sistemática de la mayoría de componentes.

5.2.1 Aplicabilidad de cada clase de mantenimiento

Supongamos un equipo en cuya constitución existan componentes cuyos fallos se produzcan agrupados en unas pocas horas al cabo de otras muchas de funcionamiento, tal y como hemos representado en la *Figura 5.1*. La curva de fiabilidad del equipo relativa al fallo de dichos componentes tendrá una disminución gradual al principio más brusca al final del periodo examinado, lo que es coherente con el incremento de la tasa de fallo al final del periodo. Si en este caso, programamos una revisión con sustitución del componente en el periodo 10 (que denominaremos tiempo medio de mantenimiento preventivo o MTMP) para el cual solo habrán fallado el 10% de los componentes, conseguiremos mantener baja la tasa de fallo y por lo tanto, mantendremos alta la fiabilidad del equipo.

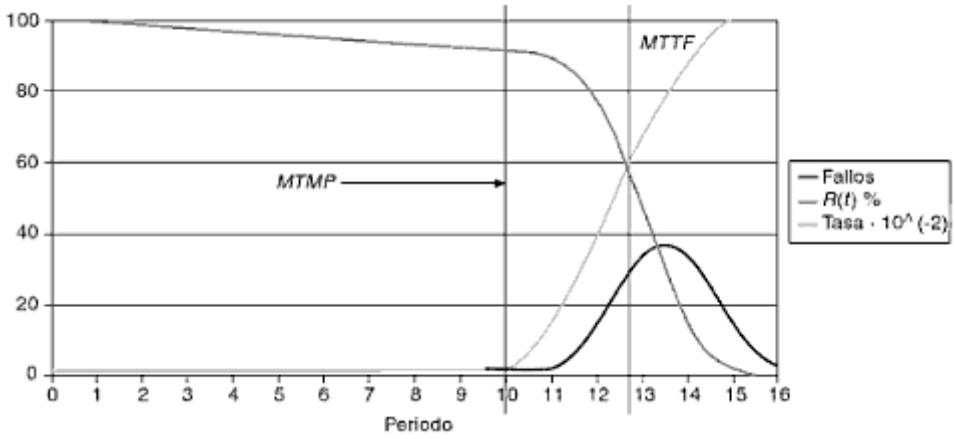

Figura 5.1: Aplicabilidad de un mantenimiento sistemático en un componente con tasa de fallo creciente.

Si el componente tiene una tasa de fallo constante, no existe un periodo en el cual su sustitución mejore la tasa de fallo del equipo; ésta permanece constante y en consecuencia, su fiabilidad también. Únicamente un mantenimiento de mejora consiste en la sustitución de los componentes por otros con una tasa de fallo menor, aumentará la fiabilidad del equipo. La *Figura 5.2* muestra un caso de este tipo.

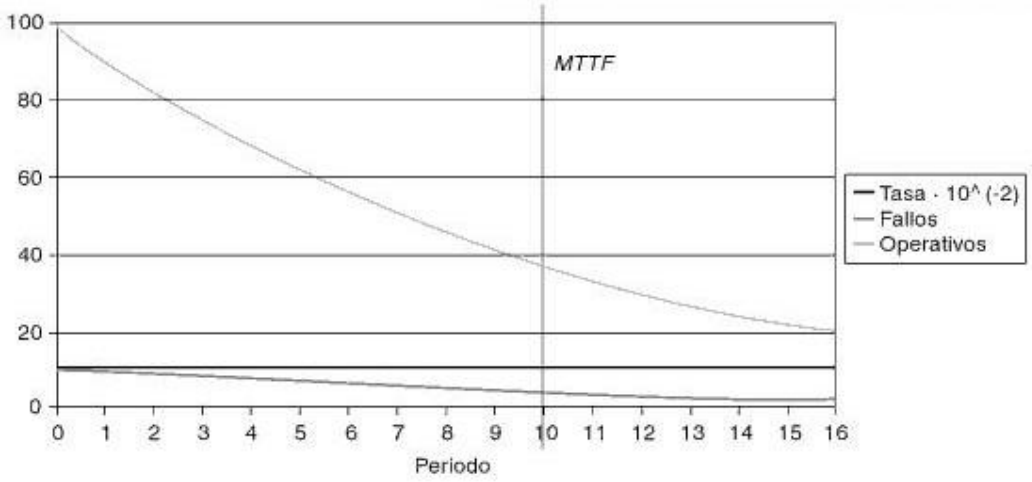

Figura 5.2. Aplicabilidad de un mantenimiento sistemático en un componente con tasa de fallo constante.

Finalmente, si el componente tiene un problema de mortalidad infantil, es decir, si se producen muchos fallos al inicio del periodo de funcionamiento y desaparecen al cabo de un cierto tiempo, la tasa de fallo disminuye con el tiempo de funcionamiento. Tal y como se representa en la *Figura 5.3*, si se realizara una sustitución del componente en un instante determinado (por ejemplo, en el instante 3), el nuevo componente aportaría una tasa de fallo mayor que la del equipo en ese momento, reduciendo así su fiabilidad; por lo tanto, tampoco en este caso las revisiones periódicas con cambios cada tiempo mejorarían la fiabilidad de la muestra, únicamente conociendo la causa de la mortalidad y actuando en consecuencia (probablemente en la fase de montaje o en la de selección de los componentes) podría disminuirse dicho problema.

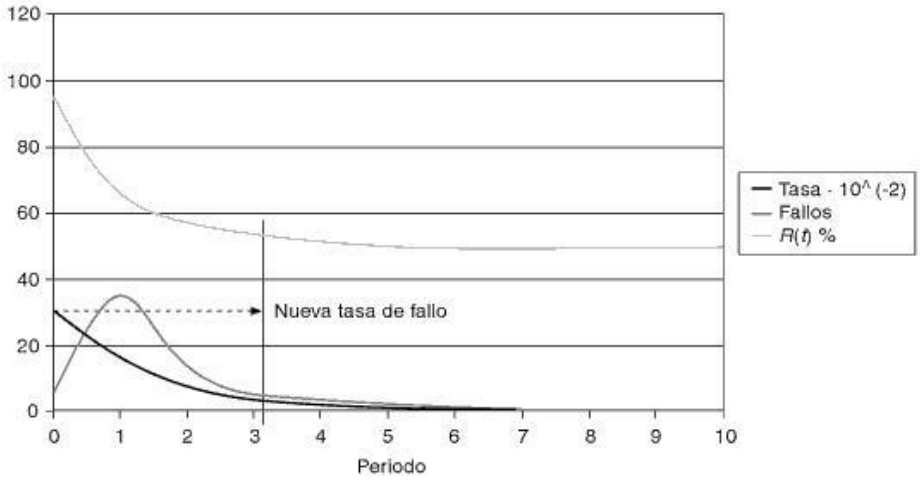

Figura 5.3: Aplicabilidad de un mantenimiento sistemático en un componente con tasa de fallo decreciente.

5.3 PREDICCIÓN DE LA MANTENIBILIDAD

La predicción de la mantenibilidad consiste en estimar la carga de trabajo asociada a cada intervención de mantenimiento al objeto de poder establecer la conformidad del diseño con los requerimientos especificados.

En el caso del mantenimiento correctivo, la predicción no es una tarea fácil porque el tiempo necesario para realizar la restauración de un equipo es suma de los tiempos exigidos por cada una de las actividades que la conforman, siendo las más importantes aquéllas que se indican en la *Tabla 5.1*. Además, está el hecho de que, las fases para la restauración de un determinado componente en un equipo concreto pueden estar afectadas por numerosos factores que aumentarán o disminuirán el tiempo inicialmente consignado. Tales factores pueden provenir del propio diseño del equipo, debido a su complejidad, peso y modularidad de los componentes, facilidad de acceso, intercambiabilidad, visibilidad, etc.; otros factores pueden ser debidos a aspectos organizativos, como el dimensionamiento de los grupos de trabajo, su grado de descentralización, la distribución de los almacenes, la calidad y disponibilidad de la documentación; finalmente, otros factores, como la existencia e idoneidad de los procedimientos de trabajo, de los útiles e instrumentos de medida, etc., pueden deberse a la práctica operativa de la empresa o centro de trabajo donde esté ubicado el equipo.

FASES	ACTIVIDADES
Diagnosis de la avería	Preparación. Localización de la avería.
Reparación	Desmontaje de los componentes con fallo. Suministro (o reparación) de los componentes necesarios. Montaje de los componentes nuevos (o reparados). Ajuste y calibrado.
Control de la reparación	Verificación del funcionamiento. Limpieza y cierre.

Tabla 5.1: Fases constitutivas de una restauración.

Por ello, la práctica más recomendable suele consistir en obtener datos a partir de la propia experiencia o de experiencias similares; cuando ello no es posible, se puede obtener una estimación del tiempo de restauración a partir de la bibliografía existente.

Una vez se conoce el $MTTR_C$ de los diversos componentes que integran un equipo, puede conocerse la mantenibilidad del mismo mediante la ecuación:

$$MTTR = \frac{\sum_e MTTR_e \cdot \lambda_e}{\sum_e \lambda_e} \quad (5.7)$$

lo que exige conocer también la tasa de fallo de cada componente.

En el caso del mantenimiento preventivo, la predicción suele ser una tarea algo menos compleja, ya que las actividades de mantenimiento suelen estar muy estandarizadas por parte de los diferentes suministradores de los componentes que integran el equipo. Aunque no suele ser muy habitual en la práctica, puede obtenerse un tiempo medio de mantenimiento preventivo MTMP a partir de los tiempos de revisión de cada componente y de las frecuencias de intervención f_e; es decir:

$$MTMP = \frac{\sum_e MTMP_e \cdot f_e}{\sum_e f_e} \quad (5.8)$$

5.4 MANTENIBILIDAD DE LOS EQUIPOS COMPLEJOS

Al igual que vimos al hablar de la fiabilidad, cuando la complejidad del equipo aumenta es conveniente descomponerlo en equipos más simples de los cuales pueda conocerse su mantenibilidad. En el diagrama de bloques resultante siempre será posible reconocer las configuraciones básicas serie y paralelo.

Configuración serie: es la configuración más habitual. Para el cálculo de la mantenibilidad se utiliza la *ecuación (5.7)*, aunque ahora, $MTMP_e$ y λ_e, son los valores de la mantenibilidad y la tasa de fallo, respectivamente, de los equipos del sistema.

Como en un sistema serie:

$$\lambda_S = \sum_{e=1}^{n} \lambda_e \quad (5.9)$$

la *ecuación (5.7)* se transforma en la:

$$MTTR_S = \frac{\sum_{e=1}^{n} \lambda_e \cdot MTTR_e}{\lambda_S} \quad (5.10)$$

la cual sugiere que el MTTR de un sistema serie puede mejorarse mediante la aplicación de los siguientes criterios:

- Disminuyendo la tasa de fallo de los componentes que tengan tiempos de restauración elevados,
- Reduciendo los tiempos de restauración de los componentes que tengan una tasa de fallo alta.

Configuración en paralelo: esta configuración, se da en equipos redundantes cuando el funcionamiento de cada uno de ellos es independiente entre sí.

6. DISPONIBILIDAD

6.1 DEFINICIÓN DE DISPONIBILIDAD

Cuando se produce un fallo en un equipo reparable éste deja de realizar las funciones para las cuales ha sido requerido hasta que se repare el fallo. Aparece, así, un nuevo concepto, la disponibilidad, que se define como la probabilidad de que un equipo realice las funciones requeridas en un instante o periodo de tiempo determinado, siempre que funcione y se mantenga de acuerdo con los procedimientos establecidos.

La disponibilidad en el instante t se representa por A(t) y para su cálculo es más práctico determinarla como complemento de la indisponibilidad, U(t), entendiendo por tal la probabilidad simultánea de que el equipo falle y además no se realice la reparación dentro del tiempo establecido; es decir:

$$U(t) = \int_0^t f(t) \cdot [1 - M(t)] \cdot dt = \int_0^t \lambda(t) \cdot [1 - M(t)] \cdot dt \qquad (6.1)$$

y de aquí:

$$A(t) = 1 - U(t) \qquad (6.2)$$

6.2 MEDIDA DE LA DISPONIBILIDAD

Si las tasas de fallo y de reparación son constantes, la *ecuación (6.2)* puede resolverse fácilmente, dando como el resultado:

$$A(t) = \frac{\lambda}{\lambda+\mu}\left[\frac{\mu}{\lambda} + e^{-(\lambda+\mu)t}\right] \qquad (6.3)$$

según la cual, en el instante inicial (t=0), la disponibilidad es máxima (A=1) y disminuye progresivamente a medida que aumenta el tiempo t; para valores de t suficientemente grandes (t=∞), la disponibilidad alcanza un valor asintótico dado por:

$$A(\infty) = \frac{\mu}{\lambda+\mu} = \frac{MTBF}{MTBF+MTTR} \qquad (6.4)$$

que es la expresión más conocida de la disponibilidad.

Si para MTBF y MTTR utilizamos las expresiones dadas en las *ecuaciones (4.8) y (*5.5*)* y las sustituimos en la *ecuación (6.4)*, tendremos:

$$A(\infty) = \frac{MTBF}{MTBF+MTTR} = \frac{\frac{t_F}{n}}{\frac{t_F}{n}+\frac{t_P}{n}} = \frac{t_F}{t_F+t_P} = \frac{t_T-t_P}{t_T} \qquad (6.5)$$

fórmula que dada su sencillez es muy utilizada en la práctica industrial y en la que: t_F representa el tiempo de funcionamiento, t_P el tiempo de paro y t_T el tiempo total ($=t_F+t_P$).

En las ecuaciones anteriores solo hemos tenido en cuenta los tiempos de reparación, lo cual es estrictamente correcto únicamente cuando el mantenimiento preventivo se realiza en periodos en los que el equipo está fuera de servicio por vacaciones, fines de semana, horas valle, horas nocturnas o por formar parte de un sistema redundante; si, en cambio, el mantenimiento preventivo se realiza en las horas hábiles de operación, deberá incluirse entonces en el cálculo de la disponibilidad. Este nuevo valor se denomina disponibilidad técnica y se calcula de la siguiente manera:

$$A_{TEC} = \frac{MTBM}{MTBM+MAMT} \qquad (6.6)$$

siendo: MTBM el tiempo medio entre acciones de mantenimiento preventivo ($MTBM_P$=MTMP) y correctivo ($MTBM_C$=MTTF) y MAMT el tiempo medio de mantenimiento activo, es decir, el tiempo medio invertido en las acciones de mantenimiento preventivo ($MTTM_P$) y correctivo ($MTTM_C$=MTTR) y que pueden calcularse mediante las expresiones siguientes:

$$\frac{1}{MTBM} = \frac{1}{MTMP} + \frac{1}{MTTF} \qquad (6.7)$$

$$\frac{1}{MAMT} = \frac{1}{MTTM_P} + \frac{1}{MTTR} \qquad (6.8)$$

Finalmente, si se tienen en cuenta los retrasos administrativos o los debidos a la falta de recambios o de personal para iniciar y continuar la actividad de mantenimiento, el nuevo valor se denomina disponibilidad operacional:

$$A_{OP} = \frac{MTBM}{MTBM+MDT} \qquad (6.9)$$

en la que MDT es el tiempo medio de paro real.

6.3 PREDICCIÓN DE LA DISPONIBILIDAD

La predicción de la disponibilidad, al ser ésta una función dependiente de la fiabilidad y la mantenibilidad, dependerá de las predicciones que se hayan hecho de las dos funciones dependientes. Si el resultado obtenido no fuera satisfactorio, entonces sería necesario corregir las predicciones realizadas para la fiabilidad y/o para la mantenibilidad hasta conseguirlo.

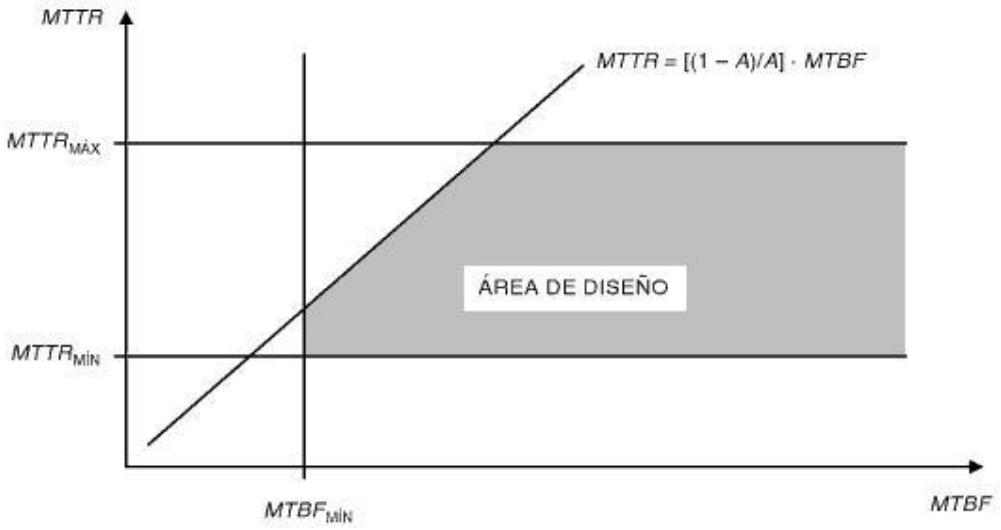

Figura 6.1: Relación entre los valores de MTTR y MTBF cuando se especifica un valor de A.

6.4 DISPONIBILIDAD DE LOS EQUIPOS COMPLEJOS

En los equipos complejos, la disponibilidad dependerá de la disponibilidad de los equipos que lo forman, de acuerdo también con las configuraciones básicas serie y paralelo.

Un **sistema serie** estará operativo únicamente cuando todos los componentes que lo forman estén operativos, por tanto:

$$A_S = \prod_i A_i \qquad (6.10)$$

también aquí, como en la fiabilidad, la disponibilidad del sistema es menor que la del componente que tenga la más baja disponibilidad.

Un **sistema paralelo** no será operativo y por tanto, no estará disponible, cuando estén indisponibles simultáneamente todos los componentes que lo forman; es decir:

$$U_S = \prod_i U_i \qquad (6.11)$$

de donde:

$$A_S = 1 - U_S = 1 - \prod U_i \qquad (6.12)$$

y por ello A_S siempre será mayor que la disponibilidad de cualquiera de los componentes que forman el sistema.

El concepto de sistema paralelo puede aplicarse no solo para calcular la disponibilidad de un equipo complejo en función de la disponibilidad de cada uno de sus componentes, sino que puede aplicarse también para garantizar la disponibilidad de una función cuando ésta sea ejecutada por uno o varios equipos independientemente, lo que resulta altamente útil para determinar el número de equipos que deberían instalarse.

7. ANÁLISIS DE LOS MODOS DE FALLO, EFECTOS Y CRITICIDAD: AMFEC (FMECA)

Todas las consideraciones cualitativas generales presentadas para el Análisis de los Modos de Fallo y sus Efectos (AMFE) se aplicarán al Análisis de los Modos de Fallo, Efectos y Criticidad (AMFEC), ya que la última es una extensión de la primera. Y debido a su generalizado uso, utilizaremos las siglas en inglés, FMEA/FMECA, *"Failure mode, effects and criticality analysis"*, para referirnos a estos análisis.

La norma por la que se rige el análisis FMEA es la UNE-EN 60812:2008 *"Analysis techniques for system reliability - Procedure for failure mode and effects analysis (fmea)".*

El FMEA es un procedimiento sistemático para el análisis de un sistema con el fin de identificar los modos de fallo potenciales, sus causas y efectos en el funcionamiento del sistema. El análisis se lleva a cabo con éxito preferiblemente en el inicio del ciclo de desarrollo, de manera que la eliminación o mitigación del modo de fallo sea lo más rentable posible. Este análisis se puede iniciar tan pronto como el sistema se haya definido lo suficiente como para presentarlo mediante un diagrama de bloques funcionales en donde se puede definir la función de sus elementos.

La aplicación del FMEA va precedida de la descomposición jerárquica del sistema en sus elementos más básicos. Es útil emplear diagramas de bloque simples para ilustrar esta descomposición (IEC 61078:2006). El análisis comienza entonces con los elementos de nivel más bajo. Un efecto de modo de fallo a un nivel más bajo puede convertirse en la causa de un fallo de un elemento en el siguiente nivel superior. El análisis continúa de abajo hacia arriba hasta que se identifica el efecto final en el sistema.

FMECA (Análisis de modos de fallo, efectos y criticidad) es una extensión del FMEA para incluir un medio de clasificar la severidad de los modos de fallo y permitir la priorización de contramedidas. Esto se hace combinando la medida de la severidad, la frecuencia de aparición y el nivel de detección para producir una métrica llamada criticidad.

El FMEA tiene que ver generalmente con modos de fallo individual y el efecto de estos modos de fallo en el sistema. Cada modo de fallo se trata de manera independiente. Por tanto, el procedimiento es inadecuado para consideración de fallos dependientes o resultantes de una secuencia de eventos. Para analizar estas situaciones se pueden requerir otros métodos y técnicas, tales como el análisis de

Markov (IEC 61165:2006) o el Análisis por Árbol de Fallos (AAF) (UNE-EN 61025:2006).

7.1 PROPÓSITOS Y OBJETIVOS DEL ANÁLISIS

Las razones para realizar un Análisis de modos de fallo y efectos (FMEA) o Análisis de modos de fallo, efectos y criticidad (FMECA) pueden incluir lo siguiente:

- Identificar los fallos que tienen efectos no deseados en la operación del sistema.
- Satisfacer los requisitos contractuales de un cliente, según sea aplicable.
- Permitir mejoras en la fiabilidad o seguridad del sistema.
- Permitir la mejora en la capacidad de mantenimiento del sistema.

Con base en las razones anteriores, como objetivos de un FMEA (o FMECA) se pueden incluir los siguientes:

- Una identificación y evaluación amplias de todos los efectos indeseados dentro de los límites definidos del sistema que se analiza, y las secuencias de los eventos provocados por cada modo de fallo del elemento identificado, cualquiera que sea su causa, a diferentes niveles de la jerarquía funcional del sistema.

- La determinación de la criticidad o prioridad para tratar/mitigar de cada modo de fallo con respecto a la función o funcionamiento correcto del sistema, y al impacto en el proceso involucrado.

- Una clasificación de los modos de fallo identificados de acuerdo con las características pertinentes, incluida su facilidad de detección, la capacidad de diagnóstico, capacidad de ensayo, compensación y disposiciones para operación (reparación, mantenimiento, logística, etc.).

- Identificación de los fallos funcionales del sistema y estimación de las medidas de la severidad, probabilidad de fallo y detección.

- Desarrollo del plan de mejora del diseño para la mitigación de los modos de fallo.

- Apoyo para el desarrollo de un plan de mantenimiento eficaz para mitigar o reducir la probabilidad de fallo.

7.2 TAREAS PRELIMINARES

7.2.1 Estructura del sistema

Es necesario incluir los siguientes elementos en la información sobre la estructura del sistema:

- Elementos del sistema diferentes, con sus características, desempeño, papel y funciones.
- Conexiones lógicas entre elementos.
- Nivel de redundancia y naturaleza de las redundancias.
- Posición e importancia del sistema dentro de la instalación completa (si es posible).
- Entradas y salidas del sistema.
- Cambios en la estructura del sistema para modos de operación variables.

La información correspondiente a funciones, características y desempeño se requieren para todos los niveles del sistema considerados, incluso hasta el máximo, de manera que el FMEA pueda abordar apropiadamente los modos de fallo que impidan cualquiera de estas funciones.

Es importante determinar el nivel de detalle que se utilizará para el análisis. Las reglas fundamentales para seleccionar los niveles de detalle del sistema para análisis dependen de los resultados deseados y de la disponibilidad de información de diseño. La selección del nivel del sistema apropiado está influenciada por la experiencia previa.

Las representaciones simbólicas de la estructura y operación del sistema, especialmente diagramas, son muy útiles como ayudas para el análisis. Como mínimo, el diagrama de bloques debería contener lo siguiente:

- Desglose del sistema en subsistemas principales, incluidas las relaciones funcionales.
- Todas las entradas y salidas marcadas apropiadamente, y los números de identificación con los cuales se referencia en forma constante cada subsistema.
- Todas las redundancias, trayectorias de señales alternativas y otras características de ingeniería que brindan protección contra fallos en el sistema.

Se debería especificar el estado de las diferentes condiciones de operación del sistema, al igual que los cambios en la configuración o posición del sistema y sus componentes durante las diferentes fases operacionales. El desempeño mínimo

exigido por el sistema se debería definir de manera que los criterios de éxito y/o fallo se puedan entender claramente. Requisitos específicos tales como disponibilidad o seguridad se deberían considerar en términos de los niveles mínimos especificados de desempeño por lograr, y los niveles máximos de daño que se van a aceptar. Es necesario tener un conocimiento exacto de:

- La duración de cada función exigida por el sistema.
- El intervalo de tiempo entre ensayos periódicos.
- El tiempo disponible para acciones correctivas antes de que ocurran consecuencias serias para el sistema.
- Todas las instalaciones, el medio ambiente y el personal, incluidas las interfaces e interacciones con operadores.
- Los procedimientos operativos durante el arranque del sistema, su apagado y otras transiciones operacionales.
- El control durante las fases operacionales.
- El mantenimiento preventivo y/o correctivo.
- Procedimientos para ensayos de rutina, si se emplean.

Se ha establecido que uno de los usos del FMEA es ayudar al desarrollo de la estrategia de mantenimiento. Sin embargo, si ésta ha sido predeterminada, se debería conocer la información sobre instalaciones de mantenimiento, equipo y repuestos, para el mantenimiento tanto preventivo como correctivo.

7.2.2 Determinación del modo de fallo

Es importante que se lleve a cabo la evaluación de todos los elementos dentro de los límites del sistema al nivel más bajo proporcional a los objetivos del análisis, para identificar todos los modos de fallo potenciales. Entonces es posible llevar a cabo una investigación para identificar todas las posibles causas de fallo y sus efectos sobre la función del sistema y subsistemas.

Los proveedores deberían identificar los modos de fallo potenciales del elemento dentro de sus productos.

7.2.3 Causas de fallo

Las causas más probables de cada modo de fallo potencial se deberían identificar y describir. Ya que un modo de fallo puede tener más de una causa, es necesario identificar y describir las causas potenciales independientes más probables.

La identificación y descripción de las causas de fallo se deberían hacer con base en los efectos de los fallos y su severidad. Cuanto más severos los efectos de los modos de fallo, con mayor exactitud se deberían identificar y describir las causas de los fallos. De lo contrario, el analista puede dedicar esfuerzos innecesarios a la identificación de las causas de los fallos de modos de fallo que tienen un efecto menor, o ningún efecto, sobre la funcionalidad del sistema.

Las causas de los fallos se pueden determinar del análisis de fallos en campo o fallos en las unidades de ensayo. Cuando el diseño es nuevo y sin precedente, las causas de los fallos se pueden establecer a partir de la opinión de los expertos.

Cuando se identifican las causas de cada modo de fallo, la acción recomendada se evaluará con base en su probabilidad de ocurrencia estimada y en la severidad de su efecto.

7.2.4 **Efectos de fallo**

Un efecto de fallo es la consecuencia de un modo de fallo en términos de la operación, función o estatus de un sistema. Un efecto de fallo puede ser causado por uno o más modos de fallo, de uno o más componentes.

Un efecto de fallo puede influir en el siguiente nivel superior y finalmente en el más alto nivel bajo análisis. Por tanto, a cada nivel se debería evaluar el efecto de los fallos en el nivel superior a éste.

Para cada modo de fallo el analista debería determinar la forma en la que se detecta el fallo y el medio por el cual el usuario o encargado del mantenimiento se entera del fallo. La detección del fallo se puede implementar por medio de una característica automática del diseño (ensayo con equipo de prueba integrado), el establecimiento de un procedimiento de inspección especial antes de la operación del sistema, o inspección durante las actividades de mantenimiento.

Para un diseño, la detección con FMEA considera qué tan probable, cómo y dónde se identificará la eficiencia de un diseño (mediante revisión, análisis, simulación, ensayo, etc.). Para un proceso, la detección con FMEA considera qué tan posible y dónde puede ser identificada una deficiencia en el proceso, y con qué probabilidad.

Otras disposiciones contra fallo que necesitan registrarse en el FMEA incluyen las siguientes:

- Elementos redundantes que permiten la operación continua si alguno de los elementos falla.
- Medios de operación alternativos.
- Dispositivos de monitoreo o de alarma.
- Cualquier otro medio que permita la operación eficaz o limite el daño.

7.2.5 Clasificación de la severidad

La severidad es una evaluación de la importancia del efecto de modo de fallo sobre la operación del componente. La clasificación de los efectos de severidad depende considerablemente de la aplicación del FMEA y se desarrolla teniendo en cuenta varios factores:

- La naturaleza del sistema en relación con los posibles efectos sobre los usuarios o el ambiente, resultantes del fallo.
- El desempeño funcional del sistema o proceso.
- Cualquier requisito contractual impuesto por el cliente.
- Requisitos de seguridad del gobierno o la industria.
- Requisitos implícitos en una garantía.

Ejemplo de un grupo de clasificación de severidad cualitativa para un producto para uno de los tipos de FMEA:

Tipo	Grado	Descripción
IV	Catastrófico	Modo de fallo que puede potencialmente dar como resultado fallo en las funciones primarias del sistema, y por tanto causa daños graves al sistema y a su ambiente, y/o lesiones personales.
III	Principal	Modo de fallo que puede potencialmente dar como resultado fallo en las funciones primarias del sistema, y por tanto causa daños considerables al sistema y a su ambiente, pero que no constituye una amenaza seria para la vida, ni presenta amenaza de lesiones personales.
II	Crítico	Modo de fallo que puede potencialmente degradar las funciones de desempeño del sistema, sin causar daño apreciable al sistema ni presentar amenazas para la vida ni lesiones personales.
I	Menor	Modo de fallo que puede potencialmente degradar las funciones de desempeño del sistema pero que no causará daño a éste ni representa una amenaza para la vida, ni lesiones personales.

Tabla 7.1: Clasificación de severidad cualitativa

7.2.6 **Frecuencia o probabilidad de aparición**

La frecuencia o probabilidad de ocurrencia de cada modo de fallo se debería determinar con el fin de evaluar adecuadamente el efecto o criticidad del modo de fallo.

Los porcentajes de fallo de los componentes y en consecuencia el porcentaje de fallo del modo de fallo que se considera, en la mayoría de casos se incrementan proporcionalmente con el incremento de los esfuerzos aplicados con la relación de ley de potencia o exponencialmente. La probabilidad de que ocurran modos de fallo para el diseño se puede estimar a partir de:

- Datos sobre el ensayo de durabilidad de los componentes.
- Bases de datos disponibles de los porcentajes de fallo.
- Datos de fallo en campo.
- Datos de fallo para elementos similares o para la clase de componente.

7.2.7 **Procedimiento de análisis**

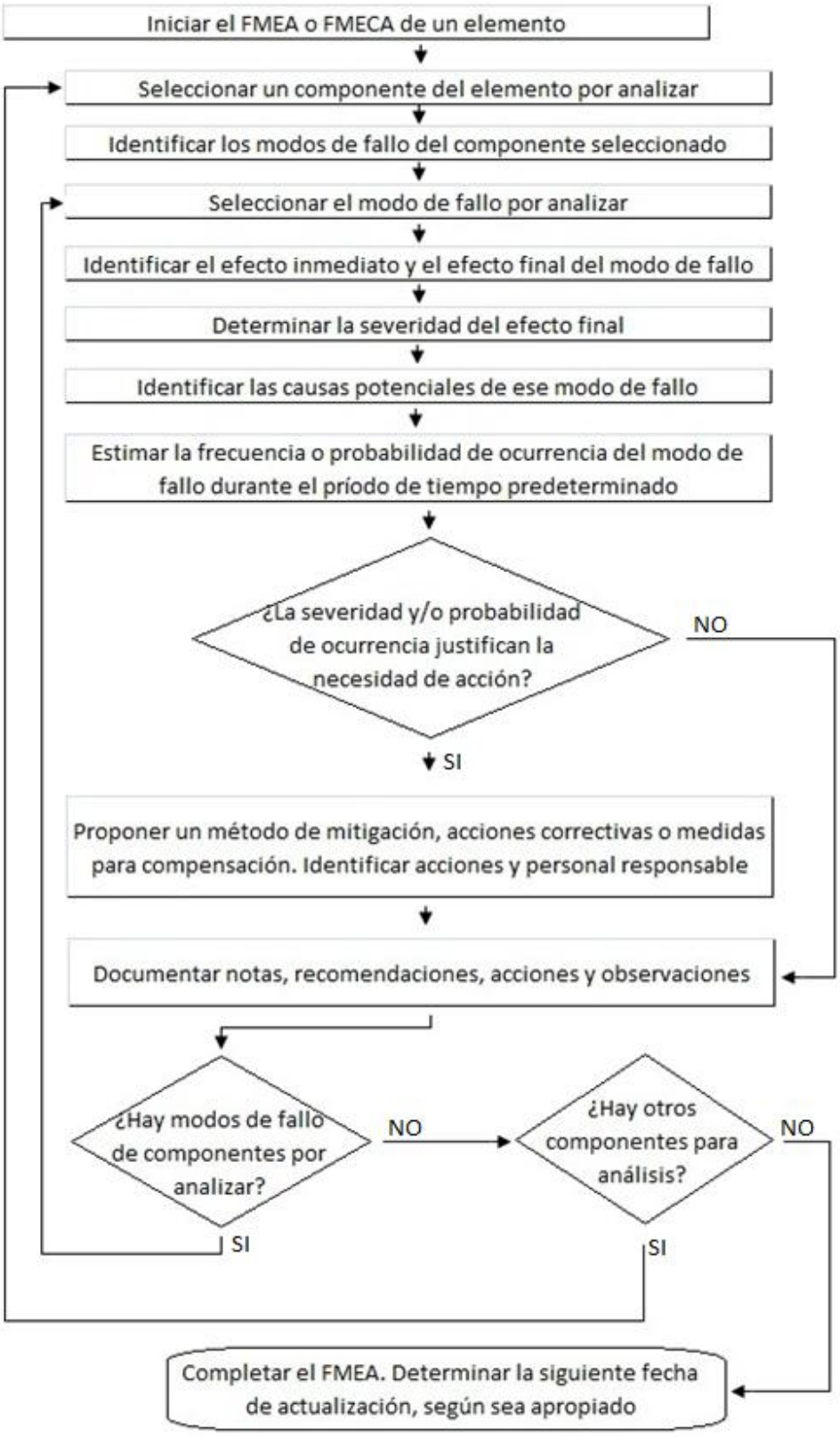

Figura 7.1: Procedimiento de análisis FMEA

7.3 ANÁLISIS DE MODO DE FALLO, EFECTOS Y CRITICIDAD (FMECA)

El propósito del análisis de criticidad es cuantificar la magnitud relativa de cada efecto de fallo como una ayuda para la toma de decisiones, de manera que con una combinación de criticidad y severidad se pueda establecer la prioridad para la acción de mitigar o minimizar el efecto de determinados fallos.

Uno de los métodos de determinación cuantitativa de criticidad es el número de prioridad del riesgo (NPR).

$$NPR = S \times O \times D \qquad (7.1)$$

en donde

S es un número no dimensional que representa la severidad, es decir, una estimación de qué tan fuerte los efectos del fallo afectarán al sistema o al usuario.

O la probabilidad de ocurrencia de un modo de fallo durante un periodo de tiempo predeterminado o establecido, aunque también puede definirse como un rango numérico más que como la probabilidad de ocurrencia real.

D significa detección, es decir, una estimación de la posibilidad de identificar y eliminar el fallo antes de que se vea afectado el sistema o el cliente. Este número se clasifica normalmente en orden inverso a partir de los números de severidad o de ocurrencia: a mayor número de detección, es menos probable la detección. La menor probabilidad de detección conduce, en consecuencia, a un mayor NPR y a una mayor prioridad para la resolución del modo de fallo.

Si hay modos de fallo con NPR similar o idéntico, los modos de fallos que se van a abordar primero son los que tengan los números de severidad mayores.

En algunas aplicaciones, los efectos con un NPR que exceden un umbral definido no son aceptables, mientras que en otras aplicaciones se da alta importancia a números de severidad altos, independientemente del valor del NPR.

Para sistemas de bajo riesgo y baja complejidad el FMECA puede ser un método muy rentable y apropiado. Siempre que durante el FMECA se reconozca la probabilidad de efectos de alto riesgo, se recomienda usar un análisis de riesgo probabilístico (ARP), en vez del FMECA.

7.3.1 Determinación de la tasa de fallo del modo de fallo, probabilidad y número de criticidad

Si las tasas de fallo para los modos de fallo de elementos similares están disponibles y fueron determinadas bajo condiciones operacionales y ambientales similares a las supuestas para el sistema que se analiza, las frecuencias de los eventos para los efectos se pueden agregar directamente al FMECA. Si las tasas están disponibles para los elementos, como es muy frecuente, en vez de para los modos de fallo, y para diferentes condiciones ambientales u operativas, es necesario calcular las tasas de fallo de los modos de fallo. En general, se establece la siguiente relación:

$$\lambda_i = \lambda_j \times \alpha_i \times \beta_i \qquad (7.2)$$

en donde

- λ_i denota la estimación de la tasa de fallo para un modo de fallo i considerado constante.
- λ_i representa la tasa de fallo del componente j.
- α_i es la razón del modo de fallo i, es decir, es la probabilidad de que el elemento tenga el modo de fallo i.
- β_i es la probabilidad condicional del efecto de fallo dado en el modo de fallo i.

Las deficiencias principales de este enfoque son la suposición implícita de la tasa de fallo constante, y que muchos de los factores son solamente predicciones o las mejores conjeturas. Éste es especialmente el caso en que los componentes del sistema no pueden tener una tasa de fallo asociada, sólo la probabilidad calculada del fallo para la aplicación específica, su duración y los esfuerzos asociados, tales como componentes y sistemas mecánicos.

En algunas aplicaciones, tales como el enfoque cuantitativo al análisis de criticidad, un número C_i de criticidad del modo de fallo se usa en lugar de la tasa de fallo, λ_i. El número de criticidad establece una conexión entre la frecuencia de fallo

condicional y el tiempo de operación, lo que puede ayudar entonces a una evaluación más realista de un riesgo de modo de fallo durante el período predeterminado de uso del producto.

$$C_i = \lambda_i \times t_j \quad (7.3)$$

$$C_i = \lambda_j \times \alpha_i \times \beta_i \times t_j \quad (7.4)$$

en donde

t_j indica el tiempo de operación del componente durante todo el tiempo predeterminado usado para el FMECA, para el cual se evalúa la probabilidad tiempo de funcionamiento del componente activo.

El número de criticidad para el componente que tiene *m* modos de fallo es entonces:

$$C_j = \sum_{i=1}^{m} \lambda_j \times \alpha_i \times \beta_i \times t_j \quad (7.5)$$

Se debe observar que el número de criticidad no está relacionado propiamente con el término criticidad. Es apenas un valor calculado para algunos tipos de FMECA en el contexto en que existe una medida relativa de la consecuencia de un modo de fallo y su probabilidad de ocurrencia. Aquí el número de criticidad es una medida de riesgo, no una medida de la probabilidad de ocurrencia.

Para determinar P_i, la probabilidad de ocurrencia del modo de fallo para un tiempo t_j, a partir de la criticidad calculada:

$$P_i = 1 - e^{-C_i} \quad (7.6)$$

En el caso de tasas de fallo o frecuencias de fallo variables, la probabilidad de ocurrencia se debe calcular, en vez de la criticidad, que se basa en la suposición de una tasa de fallo constante (frecuencia).

7.3.2 **Matriz de criticidad**

La criticidad se puede presentar en una matriz de criticidad. Debería tenerse en cuenta que no existe una definición universal para criticidad, pero es necesario que sea definida por el analista y aceptada por la dirección del proyecto o programa. Las definiciones varían ampliamente entre diferentes sectores de aplicación.

Posibilidad - probabilidad de ocurrencia					
	5				Riesgo alto
	4				
	3				
	2				
	1	Riesgo bajo			
		I	**II**	**III**	**IV**
		Severidad			

Tabla 7.2: Matriz de criticidad

7.3.3 Evaluación de la aceptabilidad del riesgo

Cuando el producto final requerido para el análisis es una matriz de criticidad, ésta puede representarse a partir de las severidades asignadas y de las frecuencias de los sucesos. La aceptabilidad del riesgo se define subjetivamente y es impulsada por decisiones profesionales y financieras, y varía en los diferentes tipos de industria. La siguiente tabla presenta algunos ejemplos de clases de aceptabilidad de riesgo y una matriz de criticidad modificada.

Frecuencia de ocurrencia del efecto de fallo	Niveles de severidad			
	1 Insignificante	**2 Marginal**	**3 Crítica**	**4 Catastrófica**
5: Frecuente	Indeseable	Intolerable	Intolerable	Intolerable
4: Probable	Tolerable	Indeseable	Intolerable	Intolerable
3: Ocasional	Tolerable	Indeseable	Indeseable	Intolerable
2: Remota	Insignificante	Tolerable	Indeseable	Indeseable
1: Improbable	Insignificante	Insignificante	Tolerable	Tolerable

Tabla 7.3: Aceptabilidad del riesgo

7.4 INFORME DE ANÁLISIS

7.4.1 Alcance y contenido de un informe

El informe sobre FMEA puede ir incluido en un estudio más amplio o puede ser independiente. En cualquier caso, el informe debería incluir un resumen y un registro detallado del análisis y los diagramas funcionales o de bloque, que definen la estructura del sistema. El informe también debería contener una lista de los dibujos en el que se basa el FMEA.

7.4.2 Resumen de efectos

Se debería elaborar un listado de los efectos de fallo en un sistema específico, resaltados por el FMEA.

Un resumen de efectos de fallo puede ser requerido para determinar la probabilidad de fallo del sistema, resultante de la lista de efectos de fallo y del establecimiento de prioridades para acciones correctivas o preventivas. El resumen de efectos de fallo se debería basar en la lista de efectos de fallos finales y debería contener detalles de la contribución de los modos de fallo del elemento a cada efecto de fallo. La probabilidad de ocurrencia de cada modo de fallo es calculada por el periodo de tiempo predeterminado de uso del elemento como por el perfil de uso esperado y los esfuerzos establecidos.

El resumen también debería contener una breve descripción del método de análisis y el nivel al cual se llevó a cabo, las hipótesis y las reglas básicas. Además, debería incluir listas de lo siguiente:

- Modos de fallo que dan como resultado efectos graves.
- Recomendaciones para diseñadores, personal de mantenimiento, planificadores y usuarios.
- Cambios de diseño que ya se han incorporado como resultante del FMEA.
- Efectos que son mitigados por los cambios de diseño incorporados.

7.5 APLICACIONES

Un usuario debería determinar cómo y para qué propósitos se usa el FMEA dentro de su propia disciplina técnica. Se puede usar solo o para complementar y apoyar otros métodos de análisis de confiabilidad. La necesidad del FMEA puede variar ampliamente de un proyecto a otro.

El FMEA apoya el concepto de revisión del diseño y se debería implementar lo antes posible en el período de diseño del sistema y subsistema. El FMEA es aplicable a todos los niveles de diseño del sistema pero es más apropiado para los niveles inferiores en donde hay involucrados grandes números de elementos y/o existe complejidad funcional. Es esencial que el personal que lleva a cabo el FMEA reciba entrenamiento especial y deben estar en estrecha colaboración con los diseñadores e ingenieros de sistemas. El FMEA se debería actualizar a medida que el proyecto avanza y que los diseños son modificados. Al finalizar el proyecto, el FMEA se usa para verificar el diseño y puede ser esencial para la demostración de conformidad de un sistema diseñado, con las normas y reglamentaciones requeridas, y con los requisitos del usuario.

7.5.1 **Beneficios del FMEA**

Algunas aplicaciones y beneficios detallados del FMEA son los siguientes:

- Evitar costosas modificaciones mediante la identificación temprana de deficiencias en el diseño.
- Identificar fallos que cuando ocurren solos o en combinación, tienen efectos inaceptables o significativos, y determinar los modos de fallo que pueden afectar seriamente el funcionamiento esperado o requerido.
- Determinar la necesidad de métodos de diseño para la mejora de la fiabilidad (redundancia, esfuerzos operativos, fallo seguro (sin daño), selección del componente y atenuación de esfuerzos, etc.).
- Suministrar el modelo lógico requerido para evaluar la probabilidad o tasa de ocurrencia de condiciones de operación anómalas del sistema en la preparación del análisis de criticidad.
- Revelar las áreas con problemas de seguridad y responsabilidad del producto o el incumplimiento de requisitos reglamentarios.
- Asegurar que el desarrollo del programa de ensayo puede detectar modos de fallo potenciales.
- Enfocarse en áreas claves en las que concentrar el control de calidad y los controles de procesos de inspección y fabricación.
- Ayudar a definir diversos aspectos de la estrategia y programa general de mantenimiento preventivo.
- Facilitar o apoyar la determinación de los criterios de ensayo, los planes de ensayo y los procedimientos de diagnóstico.
- Apoyar el diseño de secuencias de aislamiento de fallos y apoyar la planificación de modos alternativos de operación y reconfiguración.
- Brindar a los diseñadores entendimiento de los factores que influyen en la fiabilidad del sistema.
- Suministrar un documento final que demuestre que (y en qué grado) se ha tenido cuidado para asegurar que el diseño cumplirá sus especificación en servicio. (Esto es especialmente importante en el caso de la responsabilidad del producto).

7.5.2 Limitaciones y deficiencias del FMEA

El FMEA es extremadamente eficiente cuando se aplica al análisis de elementos que causan un fallo en todo el sistema o en una función importante del sistema. Sin embargo, el FMEA puede ser difícil y tedioso para el caso de sistemas complejos que tienen múltiples funciones que involucran diferentes conjuntos de componentes del sistema. Esto se debe a la cantidad de información detallada del sistema que necesita considerarse. Esta dificultad se puede incrementar por la existencia de otros modos de operación posibles, al igual que al considerar las políticas de reparación y mantenimiento.

Cualquier relación entre individuos o grupos de modos de fallo o causas de modos de fallo no se puede presentar eficazmente en el FMEA, ya que la hipótesis principal de este análisis es la independencia de los modos de fallo. La hipótesis de independencia puede hacer difícil ver un modo de fallo que puede tener consecuencias drásticas cuando es el resultado de otro modo de fallo, mientras que cada uno de ellos por separado podría tener una baja probabilidad de ocurrencia. Los escenarios de interrelación se modelan mucho mejor usando el análisis de modo de fallos con la herramienta del Análisis por Árbol de Fallos (AAF) (IEC 61025:2006).

Una deficiencia adicional del FMEA es su incapacidad para brindar una medición de la fiabilidad total del sistema y por la misma razón no puede brindar ninguna medida de las mejoras de diseño.

8. ANÁLISIS POR ÁRBOL DE FALLOS (FTA)

El análisis por árbol de fallo (AAF) o "*Fault Tree Analysis"* (FTA) (utilizaremos las siglas en inglés, FTA, por su uso más extendido) se ocupa de la identificación y análisis de las condiciones y factores que causan o que potencialmente pueden causar o contribuir a la aparición de un suceso superior definido.

El FTA se aplica a menudo al análisis de seguridad de los sistemas. También puede emplearse para análisis de disponibilidad, mantenibilidad y fiabilidad. Por simplicidad, en este apartado hablaremos de fiabilidad para representar estos aspectos del funcionamiento del sistema.

Existen dos enfoques del FTA. Uno es el enfoque cualitativo, en el que no se consideran la probabilidad de los sucesos y sus factores contribuyentes o sus frecuencias de aparición. Este enfoque consiste en un análisis detallado de los sucesos y averías y se conoce como FTA cualitativo o tradicional. El segundo enfoque es ampliamente cuantitativo, y en este caso, un FTA detallado modeliza todo un producto, proceso o sistema y la gran mayoría de los sucesos básicos, ya sean averías o no, tiene una probabilidad de ocurrencia determinada por análisis o ensayos. En este caso, el resultado final es la probabilidad de que ocurra un suceso superior que representa la fiabilidad o la probabilidad de fallo o avería.

La diferencia principal entre el FTA y otros métodos de análisis y modelización de la fiabilidad es que el FTA incluye sólo los sucesos que contribuyen a la ocurrencia del suceso superior y modeliza su combinación funcional y su posible interdependencia e interacción dinámica, mientras que otros métodos tratan con las probabilidades o tasas de fallo de los componentes (no con la probabilidad del modo de fallo del componente), con las hipótesis habituales de independencia de fallos.

8.1 DESCRIPCIÓN Y ESTRUCTURA DEL ÁRBOL DE FALLO

El árbol de fallo es una representación gráfica organizada de las condiciones u otros factores que originan o contribuyen a la aparición de un resultado definido, al que se denomina como el "suceso superior". Cuando el resultado es un éxito, entonces el árbol de fallo se convierte en un árbol de éxito, en el que los sucesos de entrada son los que contribuyen al suceso exitoso superior. La representación de un árbol de fallo debe hacerse de forma que sea claramente entendido, analizado y, si es necesario, modificado para facilitar la identificación de:

- Factores que influyen en el suceso superior estudiado.
- Factores que afectan a la fiabilidad y a las características de funcionamiento del sistema.
- Sucesos que influyen en más de un componente funcional, que podrían anular los beneficios de redundancias específicas o afectar a dos o más componentes de un producto, que podrían, de no ser así, verse como independientes o no relacionados operacionalmente.

El análisis por árbol de fallo es un método de análisis deductivo (arriba-abajo) dirigido a determinar las causas o combinaciones de causas que pueden conducir a un suceso superior definido.

Cuando no pueda estimarse la probabilidad de ocurrencia de los sucesos primarios, puede emplearse un FTA cualitativo para investigar las causas de los resultados desfavorables, marcando los sucesos primarios individuales con probabilidades de ocurrencia descriptivas, tales como: “altamente probable”, “muy probable”, “medianamente probable”, “remotamente probable”, etc.

Cuando se conocen las probabilidades de los sucesos primarios se puede utilizar un FTA cuantitativo. Entonces pueden calcularse las probabilidades de ocurrencia del suceso superior (resultado) y de todos los sucesos intermedios, de acuerdo con el modelo. También es muy útil el FTA cuantitativo para el análisis de fiabilidad de un producto o sistema durante su desarrollo.

8.2 OBJETIVOS

Puede abordarse un FTA de forma independiente o conjuntamente con otros análisis de fiabilidad. Sus objetivos incluyen:

- Identificación de las causas o combinación de causas que conducen al suceso superior.
- Determinación de si una característica particular de fiabilidad de un sistema cumple un requisito especificado.
- Determinación de qué factores o modos de fallo potenciales podrían ser los mayores contribuyentes a la probabilidad de fallo (infiabilidad) o indisponibilidad del sistema, cuando es reparable, para la identificación de posibles mejoras de su fiabilidad.

- Análisis y comparación de distintas alternativas de diseño para mejorar la fiabilidad del sistema.
- Demostración de que las suposiciones realizadas en otros análisis (tales como Markov y FMEA) son válidas.
- Identificación de modos de fallo potenciales que podrían causar un problema de seguridad, evaluación de la correspondiente probabilidad de ocurrencia y posibilidad de mitigación.
- Identificación de sucesos de causa común.
- Búsqueda de un suceso o combinación de sucesos que son los que tienen mayor probabilidad de hacer que ocurra el suceso superior.
- Evaluación del impacto de la ocurrencia de un suceso primario en la probabilidad del suceso superior.
- Cálculo de probabilidades de sucesos.
- Cálculo de disponibilidades y tasa de fallo de sistemas o de sus componentes, representados por un árbol de fallo, si se puede suponer un régimen permanente y las eventuales reparaciones son independientes unas de otras.

8.3 APLICACIONES

El FTA es particularmente adecuado para el análisis de sistemas que comprendan varias funcionalidades relacionadas o subsistemas dependientes. Sus beneficios son evidentes cuando el diseño es el resultado de varios grupos técnicos de diseño, especializados e independientes y los árboles de fallo separados se combinan. También es particularmente valioso cuando se aplica a sistemas que comprenden varios tipos de componentes (componentes mecánicos, electrónicos y software) cuya interacción no se puede modelizar fácilmente con otras técnicas.

El FTA tiene múltiples usos como herramienta, por ejemplo:

- Determinar la combinación lógica pertinente de sucesos que llevan al suceso superior y su priorización.
- Investigar un sistema en desarrollo y anticipar y prevenir, o mitigar, las causas potenciales de un suceso superior no deseado.

- Analizar un sistema, determinar su fiabilidad, identificar los principales contribuyentes a su infiabilidad y evaluar los cambios de diseño.
- Ayudar en los esfuerzos de evaluación probabilística de riesgos.

El FTA puede aplicarse a todo producto nuevo o modificado en todas las fases de diseño, como herramienta analítica para la identificación de problemas potenciales de diseño, incluyendo las fases iniciales en las que la información sobre los detalles del diseño es incompleta. Estos esfuerzos iniciales se extenderían según se vaya disponiendo de más información sobre el diseño del sistema y sus componentes. El FTA también identifica problemas potenciales que pueden proceder del diseño físico del producto, de los esfuerzos ambientales y operacionales, de defectos en los procesos de fabricación del producto y de los procedimientos de operación y mantenimiento.

8.4 FASES

Para emplear la técnica del árbol de fallo de una forma efectiva como método de análisis de sistemas, el procedimiento debería consistir al menos en las siguientes fases:

- Definición del alcance del análisis.
- Familiarización con el diseño, funciones y operación del sistema.
- Definición del suceso superior.
- Construcción del árbol de fallo.
- Análisis de la lógica del árbol de fallo.
- Realización del informe con los resultados del análisis.
- Evaluación de mejoras de la fiabilidad y compromisos.

Si se planifica realizar un análisis numérico, habrá que definir una técnica para la evaluación numérica de las probabilidades de los sucesos primarios u otros atributos, tales como intensidad de fallo, tiempo medio entre fallos (MTBF) o tiempo medio hasta el fallo (MTTF), etc.

8.5 INFORMACIÓN REQUERIDA DEL SISTEMA

El sistema que se va a analizar debería estar definido por una descripción de su función y una identificación de sus interfaces. Tal definición debería incluir:

- Un resumen del objetivo del diseño.
- Una definición de lo que constituye un fallo del sistema.
- Una estructura funcional del sistema, representada normalmente por un diagrama de bloques funcional.
- Los límites del sistema que vayan a ser regidos por las interacciones e interfaces con otros sistemas. Estos límites deberían describirse identificando las funciones particulares.
- La estructura física del sistema, en contraposición con la estructura funcional.
- Una identificación de los modos de funcionamiento del sistema, junto con una descripción de la operación del sistema y de su comportamiento esperado o aceptable en cada modo de funcionamiento.
- Un perfil operacional del sistema.
- Las condiciones ambientales del sistema y los aspectos humanos de interés.
- Una lista de documentos aplicables, por ejemplo, esquemas, especificaciones, manuales de operación, que proporcionan detalles del diseño y funcionamiento del equipo. Deberían conocerse la duración de las tareas, el intervalo de tiempo entre ensayos, así como el tiempo disponible para acciones de mantenimiento correctivo y los detalles de equipamiento de soporte y el personal implicado. También se requiere información específica sobre las funciones prescritas durante cada fase operacional.

8.6 ESTRUCTURA Y DESCRIPCIÓN GRÁFICA DEL ÁRBOL DE FALLO

Los componentes de un árbol de fallo son los siguientes:

- **Puertas**: Símbolos que muestran la relación lógica entre sucesos de entrada y el suceso de salida.
    - Puertas estáticas: El resultado no depende del orden de ocurrencia de las entradas.

    - Puertas dinámicas: El resultado depende del orden de ocurrencia de las entradas.
- **Sucesos**: nivel más bajo de entrada en un árbol de fallo.

Los componentes gráficos de un árbol de fallo son los siguientes:

- Símbolos lógicos del árbol de fallo (puertas).
- Líneas de entrada a las puertas.
- Descripciones de sucesos intermedios.
- Símbolos de transferencia de entrada o salida.
- Símbolos de sucesos primarios.

En el árbol de fallo deberían incluirse todos los sucesos de interés. Tales sucesos deberían incluir los efectos de las condiciones ambientales u otros esfuerzos a los que puede estar sometido; todos los que puedan darse durante la operación, incluso aunque estén fuera de las especificaciones de diseño.

Deberían documentarse en el informe, aunque no se incluyan en el árbol de fallo final, los sucesos que el analista haya considerado, pero que haya excluido de análisis posteriores porque los considere como no aplicables.

Si el árbol de fallo revela dos o más problemas de funcionamiento del sistema causados por un fallo existente, el suceso que describa ese fallo debería incluirse en el árbol de fallo en varios lugares. Este suceso debería marcase también como un suceso común

8.7 ALCANCE DEL ANÁLISIS

La definición del alcance del análisis debería incluir la definición del sistema que se va a analizar, el objetivo y extensión del análisis y las hipótesis básicas que se va a hacer. Estas hipótesis deberían incluir las relacionadas con las condiciones de operación y mantenimiento esperadas así como con el funcionamiento del sistema en todas las posibles condiciones de uso.

El FTA puede proporcionar información sobre:

- El análisis de la fiabilidad del sistema, en los casos en los que se conozcan las probabilidades de ocurrencia de los sucesos primarios.

- Las causas raíz de un resultado desfavorable que ha tenido lugar, que puede requerir una acción correctora adecuada.

El alcance del FTA se extiende a un sistema complejo cuando debe determinarse la probabilidad de la ocurrencia de un suceso superior. Se incluyen únicamente los modos de fallo o sucesos potenciales que influyen en el funcionamiento del sistema, es decir, se realiza una evaluación del sistema más focalizada.

8.8 DESARROLLO DEL ÁRBOL DE FALLO

El desarrollo de un árbol de fallo comienza con la definición del suceso superior o del resultado desfavorable, que debería ser definido sin ambigüedades. El suceso superior es el punto sobre el que se enfoca todo el análisis. Este suceso puede se la aparición o la existencia de una condición peligrosa (análisis de seguridad) o la incapacidad del sistema para proporcionar un funcionamiento deseado.

El desarrollo de una rama particular de un árbol de fallo termina después de que se ha producido uno o más de los sucesos siguientes:

- Sucesos primarios, esto es, sucesos independientes cuyas características pertinentes pueden definirse por medios distintos de un árbol de fallo.
- Sucesos que haya establecido el analista, que no se necesita desarrollar más.
- Sucesos que han sido o será desarrollados en otro árbol de fallo.

La modelización se realiza a través de puertas AND, OR y N/K básicamente:

- **Puertas AND (configuración en pararlelo)**

Las puertas AND se utilizan cuando existen redundancias, de manera que necesariamente se debe producir un fallo crítico en todas las alternativas para que se produzca el fallo. También se utilizan cuando dos o más modalidades de fallo no críticas, si ocurren simultáneamente, desembocan en un fallo crítico que provoca la interrupción del sistema (*ver Figura 8.1*).

Este tipo de puertas, únicamente dan fallo cuando necesariamente todas las variantes que relaciona fallan.

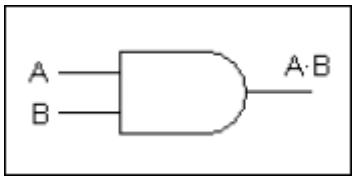

Figura 8.1: Puerta AND

Existen dos tipos de redundancias, activa y pasiva. La activa es en la que todos los componentes están activos. Y la redundancia pasiva corresponde al caso en que únicamente están activos los componentes requeridos para el funcionamiento y en caso de fallo de uno o más de ellos, se activa unos o más componentes de repuesto que asumen la función de los componentes fallados. En el análisis, puede considerarse que los componentes redundantes (repuestos) no están sometidos a fallo (repuestos fríos) o que tienen una probabilidad intermedia de fallo (repuestos templados), hasta que entran en funcionamiento activo o que están sometidos a fallo exactamente igual que cuando están en funcionamiento (repuestos calientes).

No se puede representar la redundancia en espera con puertas estáticas. Sin embargo, puede emplearse un símbolo de puerta *de repuesto*.

- **Puertas OR (configuración en serie)**

Las puertas OR se utilizan cuando cualquier fallo de alguna de las modalidades de fallo que relaciona produce la interrupción del sistema. En este tipo de puertas se encuentran todos los fallos críticos de cada componente (*ver Figura 8.2*).

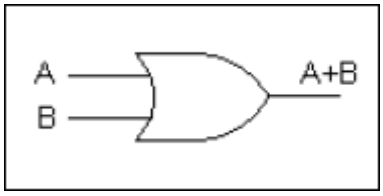

Figura 8.2: Puerta OR

- **Puertas K/N**

Las puertas K/N se utilizan para especificar a partir de qué número de fallos consecutivos se produce el fallo del sistema global. (*ver Figura 8.3*).

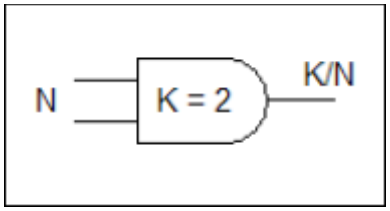

Figura 8.3: Puerta K/N

- **Sucesos repetidos (causa común) de probabilidad condicional y transferencia de sucesos al exterior**

La probabilidad condicional se da cuando la probabilidad de que tenga lugar un suceso depende de la ocurrencia de otro, donde el segundo sólo tiene lugar si el primero ocurre.

La probabilidad condicional se expresa también en términos de puertas dinámicas que usan el análisis de estado de Markov, tales como las puertas *AND de prioridad*.

8.8.1 Representación visual de árboles de fallo

Los árboles de fallo pueden representarse gráficamente de diversas formas, dependiendo de las preferencias y representaciones habituales en los distintos países y en las diferentes aplicaciones. Algunas utilizan formas rectangulares con símbolos en su interior tales como *&* para una puerta AND y ≥ para la puerta OR. En este caso, la puerta nula se clasifica también como una puerta OR, excepto que tal puerta OR sólo tiene un suceso de entrada, ya que las puertas nulas representan un suceso de salida que sólo tiene un suceso de entrada. Cuando se representan las puertas y los sucesos como rectángulos, se debería tener cuidado para asegurar que los símbolos en su interior están bien definidos y claramente marcados.

Si un suceso representa un suceso repetido o un suceso de causa común, se muestra repetidamente en el árbol de fallo, pero con una señal que indique que también se muestra como suceso de entrada para otros sucesos en el árbol de fallo. Todos los sucesos repetidos o de causa común en el conjunto deben tener el mismo código de suceso y deben estar marcados con un símbolo de entrada de transferencia o con un símbolo que se utilice normalmente para tal fin en el árbol de fallo particular.

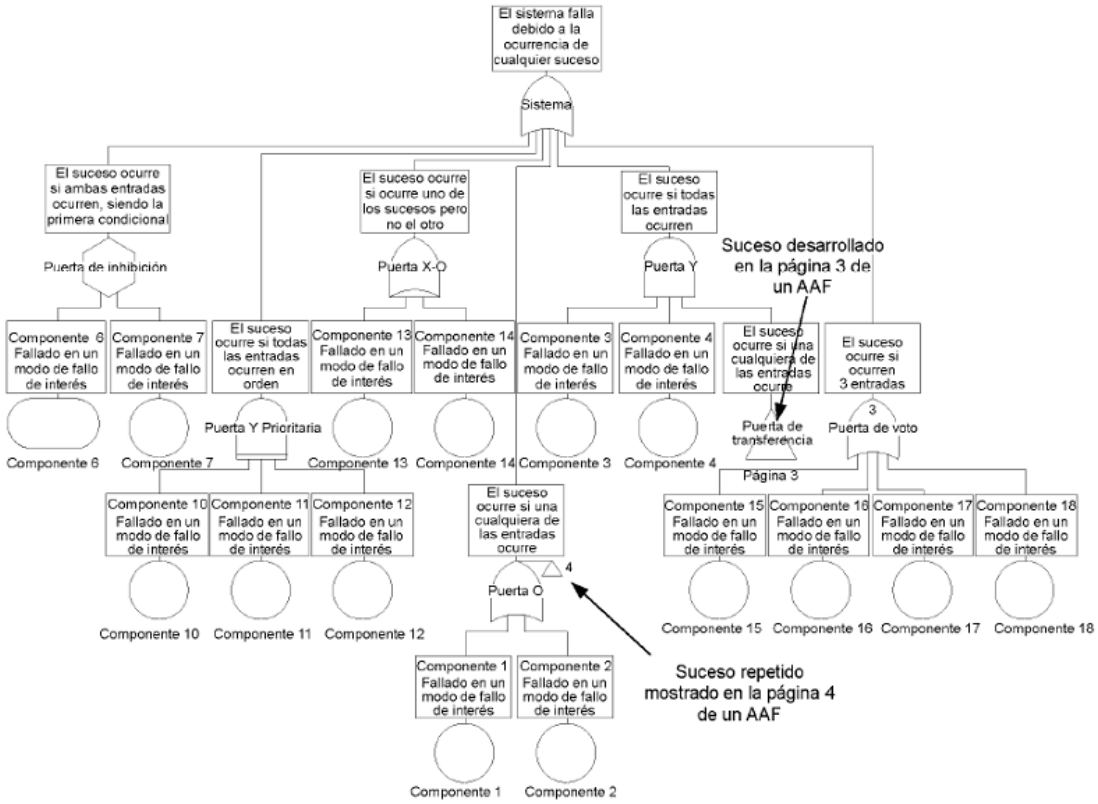

Figura 8.4: Ejemplo de árbol de fallo con un suceso repetido y un suceso de transferencia.

8.8.2 **Procedimiento de construcción**

La construcción real de un árbol de fallo sigue la lógica analítica de la secuencia de sucesos.

- El concepto de “causa inmediata” requiere que el analista determine las causas inmediatas, necesarias y suficientes, para la ocurrencia del suceso superior. Debería señalarse, que estas no son las causas básicas del resultado o suceso superior, pueden ser los sucesos de nivel inferior (intermedios).

- Las causas inmediatas, necesarias y suficientes, del suceso superior, se tratan ahora como sucesos intermedios y el análisis prosigue para determinar sus causas inmediatas (sucesos de entrada) necesarios y suficientes.

- La construcción continúa hacia abajo en el árbol, hasta alcanzar finalmente el nivel de resolución adecuado o definido. Los sucesos básicos individuales o primarios (abajo) son los que representan causas individuales de fallos o averías potenciales.

8.9 EVALUACIÓN DEL ÁRBOL DE FALLO

La evaluación del árbol de fallo puede ser lógica (cualitativa), numérica (cuantitativa) o ambas. El análisis de un árbol de fallo cuantitativo utilizado en el desarrollo de un producto para mejorar su fiabilidad, identifica los factores que contribuyen de forma importante a la probabilidad de que ocurra el suceso superior y las causas de aquéllos que tienen una alta probabilidad de ocurrencia.

Los objetivos principales de los análisis lógico (cualitativo) y numérico (cuantitativo) de un sistema pueden resumirse en los siguientes:

- Identificación de sucesos o fallos que pueden causar directamente un fallo de un sistema y contribuir a la probabilidad de tales sucesos y, de esta forma, mejorar la fiabilidad de un sistema.
- Mitigar los fallos que pueden contribuir a resultados que pueden ser riesgos potenciales de seguridad.
- Evaluación de la tolerancia a fallos del sistema (capacidad para funcionar incluso después de la aparición de un número de fallos o sucesos de nivel inferior que contribuyen a la ocurrencia de un fallo del sistema).
- Evaluación de información para localizar componentes críticos y mecanismos de fallo.
- Identificación de diagnósticos de fallo de dispositivos, información de entrada para las estrategias de reparación y mantenimiento, etc.

8.9.1 Análisis lógico

Para el análisis lógico se utilizan tres técnicas básicas: estudio, reducción booleana y determinación de cortes mínimos. La base del análisis lógico es la modelización. Una modelización correcta supone representar las funciones o componentes de un sistema de forma que se establezcan sus interacciones, dependencias, causas inmediatas de resultados desfavorables, etc.

La **reducción booleana** puede emplearse para la evaluación de los efectos de los sucesos de causa común (sucesos idénticos que ocurren en ramas diferentes) en árboles de fallo en los que la ocurrencia del suceso superior no depende del tiempo y de la secuencia de los sucesos.

Hay varios métodos para determinar **cortes mínimos**, pero su aplicación en árboles grandes puede ser difícil e incompleta. Por esta razón, existen distintos programas informáticos para ayudar al analista.

Un corte es un grupo de sucesos que cuando suceden conjuntamente, hacen que ocurra el suceso superior. Un corte mínimo es el más pequeño de estos grupos, en el que tienen que ocurrir todos los sucesos para que ocurra el suceso superior. Cuando la aparición del suceso superior depende de la secuencia de los sucesos de entrada, este suceso se analiza utilizando técnicas de Markov (IEC 61165:2006).

8.9.2 Análisis numérico

La finalidad del análisis numérico es proporcionar una evaluación cuantitativa de la probabilidad de que ocurra el suceso superior o un conjunto seleccionado de sucesos. También puede emplearse para apoyar y complementar el análisis lógico. Para realizar una evaluación numérica de un árbol de fallo se necesitan datos probabilísticos a nivel componente.

8.10 TASAS DE FALLO EN EL ANÁLISIS POR ÁRBOL DE FALLO

En muchos casos, el análisis por árbol de fallo puede utilizar tasas de fallo en vez de probabilidades de fallo de sucesos. En este caso se supone que la distribución Poisson es aplicable para caracterizar la ocurrencia de los sucesos y que las tasas de fallo asociadas son constantes. El suceso superior resultante se representa también por su tasa de fallo.

8.11 IDENTIFICACIÓN Y ETIQUETADO EN UN ÁRBOL DE FALLO

Cada suceso en un árbol de fallo debe identificarse de una forma única. Los sucesos deberían etiquetarse de forma que pueda realizarse fácilmente una referencia cruzada entre el árbol de fallo y la documentación de diseño correspondiente.

El suceso superior del árbol de fallo es un resultado no deseado, que constituye la razón principal por la que se emprende el análisis. Debería indicarse que únicamente puede asociarse un suceso superior a un árbol de fallo dado.

En un árbol de fallo, si varios sucesos se refieren todos a diferentes modos de fallo del mismo elemento, deben etiquetarse tales sucesos de forma que se les pueda distinguir. Al mismo tiempo, debería quedar claro que son un grupo de sucesos relacionados con el mismo elemento.

Si un suceso en particular ocurre en varios lugares de un árbol, o en varios árboles, todas estas ocurrencias deben llevar la misma etiqueta.

Un código típico de sucesos debería contener información relativa a la identificación del subsistema, para la identificación de un componente y de su modo de fallo.

8.12 INFORME

El informe sobre el análisis por árbol de fallo debería incluir como mínimo, los elementos básicos que indican más abajo. Puede proporcionarse información adicional y complementaria para aumentar la claridad, especialmente en el caso de análisis de sistemas complejos.

Los elementos básicos del informe deberían ser los siguientes:

- Objetivo y alcance.
- Descripción del sistema: descripción del diseño, operación del sistema, definiciones detalladas de los límites del diseño.
- Suposiciones: suposiciones del diseño del sistema.
- Suposiciones de operación, mantenimiento, inspección y ensayo, suposiciones de modelización de la fiabilidad y disponibilidad.
- Analista/equipo de analistas con conocimientos y experiencia aplicable, establecida en la cabecera o en una sección separada del informe: definición y criterios del suceso superior.
- Referencias para los sucesos básicos, sucesos no desarrollados y sucesos analizados en otra parte, por ejemplo, en diferentes proyectos y justificación del uso de sus probabilidades (por ejemplo, mismo esfuerzo, mismo perfil de utilización, etc.).
- Análisis por árbol de fallo: análisis, datos, símbolos empleados, fallos de causa común, cuando sea apropiado, cortes mínimos, cuando sea apropiado.
- Resultados, conclusiones y recomendaciones.

Pueden incluirse los siguientes datos complementarios:

- Diagrama de bloques del sistema o diagramas de los circuitos.

- Resumen de los datos de fiabilidad y mantenibilidad y fuentes utilizadas.
- Análisis FMEA/FMECA o referencia para el análisis.

La tabla del FMEA puede ser un método útil para la representación de un asunto, sugerencias para mejora del diseño, sugerencias para la verificación de un asunto, tal como un ensayo, y para el seguimiento de esas actividades.

9. MODELO GENERAL PARA ELABORAR UN ANÁLISIS RAMS

El proceso de aplicación de la tecnología RAMS se realiza al inicio del proyecto, en las fases de diseño, fabricación, ensayo e instalación y en la operación, mantenimiento y finalización de la vida útil del producto.

9.1 CONSIDERACIONES GENERALES

El cálculo de la fiabilidad del sistema se realizará teniendo en cuenta que:

- No se consideran los daños causados por terceras personas.
- Todos los fallos de los componentes se consideran independientes entre sí y de aparición aleatoria.
- Se considera que los sistemas funcionalmente relacionados con el estudio, funcionan correctamente.
- El estudio de fiabilidad se realiza desde un punto de vista conservador, es decir, que los resultados tienden a ser pesimistas.
- Se considera que todos los elementos son reparables.

9.1.1 Tasas de fallo y reparabilidad

Esta actividad consiste en la asignación de las tasas de fallo y reparación de los componentes o equipos que conforman el sistema, así como la revisión de los planes de mantenimiento planificados y no planificados. Para esta etapa se realizan los siguientes pasos:

- **Recopilación de Data Histórica Propia**: muchas empresas buscando la mejora continua de sus procesos han hecho grandes esfuerzos en la recolección de información de campo sobre datos de fallo (tipo y frecuencia) y datos de reparación de sus equipos. La cantidad y calidad de este tipo de información son de gran importancia para este estudio pues reducen los valores de incertidumbre en el análisis.
- **Recopilación de Opinión de Expertos**: existen casos donde no se cuenta con suficiente información de campo, y en ausencia de ella existen metodologías que permiten la recolección de información a partir de opinión de experto.

- **Búsqueda y adecuación de Información Genérica**: con la finalidad de obtener resultados fiables, es extremadamente importante complementar la información de fallos propia del sistema, con datos de fiabilidad genéricos provenientes de reconocidas bases de datos internacionales como OREDA(1), PARLOC(2), WELL MASTER(3), IEEE(4) y SINTEF(5). Sin embargo, es vital adecuar esta información al entorno operacional bajo análisis, seleccionando de las bases de datos, solo aquellos modos de fallos que puedan realmente ocurrir en el entorno bajo estudio.

- **Revisión y Validación de las Bases de Datos**: En esta etapa, un equipo de trabajo dirige sus esfuerzos en validar la información de fiabilidad para cada elemento del sistema (MTTF y MTTR). Esta etapa incluye un conjunto de entrevistas formales de trabajo con personal asociado al proceso productivo (operadores, analistas, programadores, ingenieros de procesos), con la finalidad de intercambiar y aclarar las premisas referentes a la base de datos, y de revisar y definir la filosofía de operaciones del proceso productivo bajo estudio. Esto incluye la revisión de los P&ID(6), diagramas funcionales, diagramas de proceso, registros de operación y fallos, planes de mantenimiento y otras fuentes de información para complementar el análisis.

- **Estimaciones**: la información proveniente de los pasos anteriores se utiliza para obtener una estimación representativa de las tasas de fallo y reparación característica del sistema o proceso. Esto se logra formulando relaciones algebraicas que permita usar distribuciones de probabilidad y fundamentos de matemática Bayesiana, para combinar la evidencia con información genérica.

(1) OREDA: Offshore Reliability Data.
(2) PARLOC: Pipeline And Riser Of Containment.
(3) WELL MASTER: Información hidrogeológica en pozos de agua para pozos y perforaciones.
(4) IEEE: Institute of Electrical and Electronics Engineers.
(5) SINTEF: "Fundación para la investigación científica e industrial" en Instituto de la tecnología noruego (NTH).
(6) P&ID: Piping and Instrumentation Diagram (Diagramas de procesos e instrumentación).

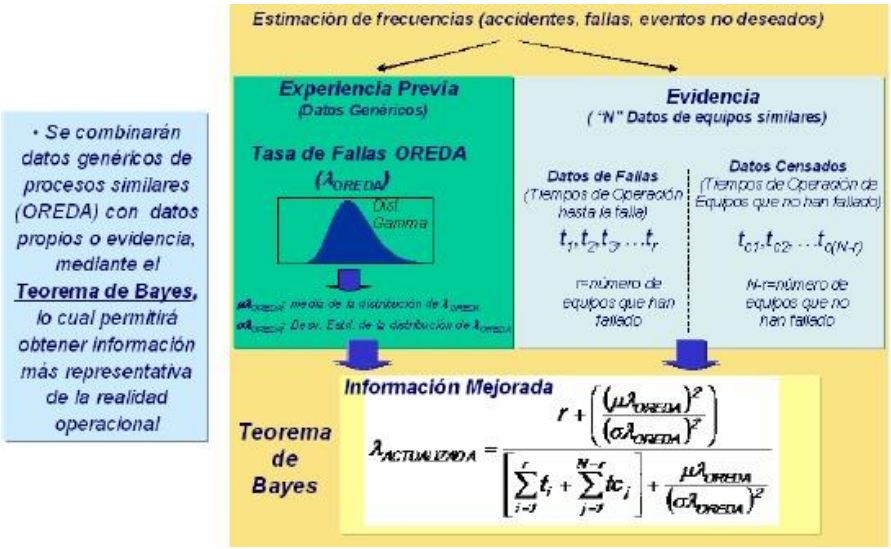

Figura 9.1: Modelo de Actualización de Tasas de Fallo

9.2 ETAPAS

Las etapas se realizan gradualmente con un conocimiento cada vez más profundo del sistema hasta llegar a la última etapa en la que se comparan los valores obtenidos con los objetivos iniciales establecidos. Si algún objetivo no se cumple, es necesario repetir al análisis, a no ser que se tome la decisión de disminuir las exigencias especificadas inicialmente para el sistema.

Para mayor entendimiento, explicaremos estas etapas apoyándonos en todo momento en un ejemplo simplificado (*Puertas automáticas de un vagón de una línea de metro con cierre de andenes*).

9.2.1 Descripción del ejemplo Puertas automáticas de un vagón de una línea de metro con cierre de andenes[(1)]

Las puertas automáticas para el cierre de andenes de estaciones, también denominadas PSD (*Platform Screen Doors*), suponen un aumento en la seguridad de los usuarios del mismo y, a la vez, proporciona un aislamiento acústico entre el tren y el andén.

El sistema de cierre de andenes está formado por paneles fijos y puertas de apertura y cierre automáticas en la plataforma del andén sincronizadas con las puertas del vagón cuando éste para en la estación.

En el estudio se considera un vagón con dos puertas que son accionadas automáticamente y de forma sincronizada con las puertas de los paneles fijos de la plataforma del andén mediante la Unidad de Control de Puertas (UCP) situada en el andén y que se comunica con éste a través del equipo de transmisión de señales tren-

(1) Creus Sole, Antonio (2005). *Fiabilidad y Seguridad*.

andén. No se consideran modos degradados de funcionamiento tales como la inhabilitación de una puerta o la del equipo de transmisión de señales entre el tren y el andén o la conducción, en modo manual, por personal embarcado.

Cuando el tren llega a la estación, la unidad de control de puertas (UCP) del andén establece comunicación con el tren, detecta el paro del mismo en la posición exacta (puertas del vagón frente a puertas del andén) y, a través del equipo de transmisión tren-andén, envía la orden de apertura selectiva de puertas. Cuando finaliza el tiempo programado, la UCP envía la señal de cierre selectivo de puertas, éstas se cierran y al recibir la señal de puertas cerradas, el tren arranca.

El funcionamiento es más complicado de lo descrito en esta aplicación simplificada, ya que la secuencia indicada debe ser aprobada por el programa de seguridad del sistema cuya finalidad es identificar y resolver los riesgos que pueden presentarse.

La puerta automática funciona del modo siguiente:

La puerta está formada por dos hojas correderas movidas por una correa dentada accionada directamente por dos motores de inducción trifásicos dotados de piñones.

El mecanismo de bloqueo de la puerta en posición de cierre consiste en un sistema de rampa que actúa al final del carril de rodadura y un mecanismo pivotante que garantiza el enclavamiento seguro de las dos hojas de la puerta. La información de la posición de cierre y enclavamiento viene dada por cuatro finales de carrera (dos por hoja).

El control funcional de la puerta se realiza mediante dos autómatas programables (PLC) alimentados con dos líneas de alimentación diferentes que actúan sobre dos módulos. Estos utilizan un convertidor de frecuencia que regula la frecuencia y tensión de salida mediante la técnica de modulación PWM, lo que permite conocer la velocidad y el par instantáneos de cada motor gracias a un codificador.

Se consideran tres clases de fiabilidad en el tren:

- Fiabilidad básica – MTBF (Tiempo medio entre fallos). Fallos que requieren una acción correctora de mantenimiento o la intervención del personal de explotación para restablecer la funcionalidad del sistema.

- Fiabilidad servicio no vital – MTBF (Tiempo medio de buen funcionamiento). Fallos que obligan a intervenir al personal de mantenimiento, sin afectar al servicio ni a su seguridad.

- Fiabilidad servicio vital – MTBSF (Tiempo medio entre fallos que afecten al servicio). Fallos que provocan un retraso en el servicio (típicamente de 2 minutos, 15 minutos o mayor)

9.2.2 **Etapa 1: Plan RAM**

- **Objetivos establecidos de fiabilidad, disponibilidad y mantenibilidad.**

Objetivo de la fiabilidad = $8 \cdot 10^{-5}$ fallos/hora

Objetivo de disponibilidad = 0,9999

Objetivo de mantenibilidad: MTBF = 14.500 horas, MTTR ≤ 15 minutos

- **Definición de las categorías de los fallos**

	FIABILIDAD BÁSICA - MTBF (Tiempo medio entre fallos). Fallos que requieren una acción correctora de mantenimiento o la intervención del personal de explotación para restablecer la funcionalidad del sistema.				**Gravedad de los Fallos**			
Pos.	**Fallo**	**Fallos/h · 10E6**	**MTTR (min)**	**Efectos**	**I Catastr**	**II Crítico**	**III Marginal**	**IV Insignific**
1	Una puerta no cierra de forma automática.	5,00	8	Alarma en cabina mando - Cerrar manualmente.			#	
2	Una puerta no abre de forma automática.	6,00	4	Alarma en la cabina - Abrir manualmente.				#
3	Falla el bus de comunicaciones.	4,50	5	Alarma en la cabina - Accionar.				#
4	Falla una línea de alimentación eléctrica.	8,00	6	Aviso al conductor. Línea 2 alimenta.				#
	FIABILIDAD SERVICIO NO VITAL - MTBF (Tiempo medio de buen funcionamiento). Fallos que obligan a intervenir al personal de mantenimiento, sin afectar al servicio.				**Gravedad de los Fallos**			
Pos.	**Fallo**	**Fallos/h · 10E6**	**MTTR (min)**	**Efectos**	**I Catastr**	**II Crítico**	**III Marginal**	**IV Insignific**
1	Módulo de control de la puerta fuera de servicio.	1,80	5	Alarma en UCP.				#
2	Fallo del sistema de señalización óptico.	0,05	5	Disminución de la luminosidad.				#
3	Fallo del sistema de señalización acústico.	0,06	3	Pérdida de señalización				#
4	UCP fuera de servicio.	5,00	4	Sin posibilidad accionamiento manual de UCP.				#

	FIABILIDAD SERVICIO VITAL - MTBSF (Tiempo medio entre fallos que afecten al servicio). Fallos que provocan un retraso en el servicio típicamente entre 2 y 15 minutos.				Gravedad de los Fallos			
Pos.	**Fallo**	**Fallos/h · 10E6**	**MTTR (min)**	**Efectos**	**I Catastr**	**II Crítico**	**III Marginal**	**IV Insignific**
1	Fallo alimentación eléctrica tiempo > 15 min.	2,60	10	Las puertas no abren de forma automática.			#	
2	Módulo accionamiento puerta fuera.	1,50	8	Alarma en la cabina.				#
3	UCP fuera de servicio.	15,00	6	Accionamiento manual del conductor.				#
4	Atrapamiento de ropa del usuario.	1,50	10	PLC capta sobrecarga motores y abre puertas.			#	

Tabla 9.1: Plan RAM

Lo primero es dividir los modos de fallo según la clase de fiabilidad a la que correspondan, 'fiabilidad básica', 'fiabilidad servicio no vital' o 'fiabilidad servicio vital'. Describir los modos de fallo y sus efectos, la tasa de fallos, el MTTR (Tiempo medio para reparar) y la gravedad de los fallos. En la siguiente tabla se describen los grados de gravedad de los fallos.

Tipo	Grado	Descripción
I	Catastrófico	Muertes y daños materiales y medioambientales muy importantes.
II	Crítico	Lesiones graves a personas y daños materiales y medio ambientales importantes.
III	Marginal	Lesiones leves a personas y daños materiales y medio ambientales menores.
IV	insignificante	Sin lesiones a personas ni daños materiales ni medioambientales.

Tabla 9.2: Categoría del riesgo

9.2.3 **Etapa 2 : Análisis preliminares. FMECA, FA, PHA Y PAA**

Para la realización de análisis RAMS es necesario un amplio entendimiento del funcionamiento del sistema, por lo que hay que añadir toda la información que facilite este entendimiento, como esquemas eléctricos, electrónicos y mecánicos.

No disponemos de esquemas sobre el caso que estamos utilizando de ejemplo.

- **Análisis de Modos de Fallo y de sus Efectos (FMEA)**

En este aparatado se realiza una breve descripción del Análisis de modos de fallo y de sus efectos, aunque podrá encontrar una descripción más extendida en el *apartado 7* de este documento.

El análisis FMEA (Failure Mode and Effects Analysis) sirve para determinar los componentes críticos, la justificación de los diseños escogidos y las calificaciones y acciones de calidad que aseguren los requerimientos de los subsistemas. El análisis mejora la tasa de fallos al permitir, si se cree conveniente, tomar decisiones en la mejora de la calidad de los componentes y, por lo tanto, en su disponibilidad.

Este método sigue una aproximación inductiva, partiendo del conjunto de los eventos peligrosos o de fallo de los componentes o piezas y siguiendo el sistema hacia adelante, buscando todas las consecuencias posibles de los sucesos de fallo.

El análisis FMEA puede ser incluso más detallado que un árbol de fallos, ya que debe considerarse cada tipo de fallo de cada componente.

Debido al gran detalle que ofrece este método, deben prepararse listas de comprobación para cada tipo de equipo o de sistema.

El nivel de riesgo se determina por la fórmula:

RIESGO = Probabilidad de fallo * Grado de severidad

NIVEL	PROBABILIDAD	DESCRIPCIÓN	CLASE DE FALLO INDIVIDUAL
A	10^{-1}	Frecuente	Ocurre con frecuencia.
B	10^{-2}	Probable	Ocurre varias veces durante la vida útil.
C	10^{-3}	Ocasional	Ocurre alguna vez en la vida útil del componente.
D	10^{-4}	Remoto	Es difícil que ocurra pero cabe la posibilidad.
E	10^{-5}	Improbable	Es muy difícil que ocurra.

Tabla 9.3: Probabilidad de fallo

Tipo	Grado	Descripción
I	Menor	Fallo potencial de alguna parte del sistema, sin lesiones al personal.
II	Crítico	El fallo ocurrirá sin daños importantes al sistema.
III	Principal	Daños importantes en el sistema y lesiones serias al personal.
IV	Catastrófico	Pérdida completa del sistema y muerte potencial.

Tabla 9.4: Grado de severidad

Y, a partir de estos datos, puede prepararse una matriz de riesgo:

Nivel de Probabilidad	A - Frecuente -(10^{-1})	-	-	PR1	-
	B - Probable -(10^{-2})	-	PR2	-	Alto riesgo
	C - Ocasional -(10^{-3})	PR3	-	Medio riesgo	-
	D - Remoto -(10^{-4})	-	Bajo riesgo	-	-
	E - Improbable -(10^{-5})	-	-	-	-
	-	I - Menor	II - Crítico	III - Principal	IV - Catastrófico
		Grado de severidad (PR = Prioridad de riesgo)			

Tabla 9.5: Ejemplo de matriz de riesgo

Nº.	Descripción	Ud.	Función	Modos de fallo		Causas de fallo
				Generales	Genéricos	
1	**ARMAZÓN**	1	-	-	1	-
1.1	Perfil principal y caucho rodadura	1	Guía y soporte carros y tope ruedas	4	1	Defecto fabricación
2	**MOTORIZACIÓN**	1	-	-	-	-
2.1	Correa	1	Transmis. movim. a las hojas	4	1	Defecto fabricación
2.2	Codificador motor	1	Posición eje motor	4	18	Defecto fabricación
2.3	Grupo electrónico	1	Control sistema	4	30, 31, 32	Vibraciones - ajuste defectuoso
2.4	Motor completo	1	Movimiento y potencia a correa	4	18, 19, 20	Vibraciones - ajuste defectuoso
2.5	Cable alimentación	1	Energía al sistema	4	1, 32	Falla red
3	**HOJA DER., IZQ.**	1	-	-	-	-
3.1	Poleas de traslación	7	Movilización carro sobre guías	4	2	Desgaste
3.2	Tope caucho	1	Rotación chapa	4	1	Desgaste
3.3	Chapa leva de accionamiento	1	Accionamiento microrruptor	4	2, 4, 18	Desgaste, Vibraciones
4	**GRUPO PLC**	1	SCHNEIDER o similar	4	15, 18, 26, 27, 28, 29, 30, 31, 32	Avería
5	**CHAPA CENTRAL**	1	-	-	-	-
5.1	Chapa central	1	Soporte y centrado del microrruptor	4	1, 2, 3	Vibraciones
5.2	Tope de caucho	2	Tope movim. carros izq. y der.	4	1	Desgaste
5.3	Microrruptor	4	Sensor contacto cierre y apertura puertas	4	2, 5, 6, 7, 8, 21, 30, 31	Avería
5.4	Enclavamiento mecánico	2	Enclavam. Cierre puertas por movim. Gatillo	4	1, 2	Desgaste

Tabla 9.6: Análisis previo FMECA

Nº.	Consecuencias del fallo		Detección del fallo	Dispositivos alternativos	Probabilidad de fallo					Nivel de criticidad			
	Efecto local	Efecto final			Muy baja	Baja	Media	Alta	Muy Alta	I	II	III	IV
1	-	-	-	-									
1.1	Bloqueo puerta	Puerta inoperativa	Micros	-	X						X		
2	-	-	-	-	X								
2.1	Puertas móviles	Puerta inoperativa	Micros	-	X						X		
2.2	-	-	Mantenimiento	El otro motor	X					X			
2.3	Motor inoperativo	-	Autómata	El otro grupo electrónico		X				X			
2.4	Motor inoperativo	-	Autómata	El otro motor	X					X			
2.5	Puerta inoperativa	Puerta inoperativa	Micros	UCP		X				X			
3	-	-	-	-									
3.1	Puerta inoperativa	Puerta inoperativa	Micros	-	X					X			
3.2	-	-	Mantenimiento	-	X					X			
3.3	Fallo cierre	Puerta inoperativa	Micros	-	X					X			
4	Motor no funciona	-	UCP	-		X				X			
5	-	-	-	-									
5.1	Micros no van	Puerta inoperativa	Micros	-	X					X			
5.2	Ruido	Desgaste enclavam.	Mantenimiento	-	X					X			
5.3	PLC no recibe señal	-	PLC	El otro PLC		X				X			
5.4	Fallo micro	Micros inoperativos	PLC	-	X					X			

Tabla 9.7: Análisis previo FMECA (cont.)

Un análisis FMEA siempre ha de llevar la descripción y función de cada componente, los modos y causas de fallo y las consecuencias del fallo, pudiéndolas dividir en efectos locales, efectos en el siguiente nivel superior, y efectos finales. También hay que detallar el modo en el que se detectan los fallos, los dispositivos alternativos existentes, la probabilidad de fallo y el nivel de criticidad.

Los modos de fallo que se utilizan no son siempre los mismos para todos los análisis FMEA. Cada sistema con sus respectivos componentes tienen sus propios modos de fallo y éstos pueden estar descritos en la norma específica del sistema o simplemente detallado en el informe del análisis por el analista.

En este caso, los modos de fallo que hemos utilizado son:

Modos de fallo generales:

Modo	Descripción
1	Funcionamiento prematuro
2	No funciona en el instante previsto
3	No deja de funcionar en el instante previsto
4	Fallo durante el funcionamiento

Tabla 9.8: Modos de fallo generales

Modos de fallo genéricos:

Modo	Descripción	Modo	Descripción
1	Fallo estructural (rotura).	**18**	Falsa actuación.
2	Bloqueo físico o atasco.	**19**	No se para.
3	Vibración.	**20**	No arranca.
4	No se queda en posición.	**21**	No conmuta.
5	No se abre.	**22**	Funcionamiento prematuro.
6	No se cierra.	**23**	Funcionamiento retardado.
7	Fallo en posición abierta.	**24**	Entrada errónea (aumento).
8	Fallo en posición cerrada.	**25**	Entrada errónea (disminución).
9	Fugas internas.	**26**	Salida errónea (aumento).
10	Fugas externas.	**27**	Salida errónea (disminución).
11	Excede la tolerancia superior.	**28**	Pérdida de la entrada.
12	Excede la tolerancia inferior.	**29**	Pérdida de la salida.
13	Funcionamiento inadvertido.	**30**	Cortocircuito (eléctrico).
14	Funcionamiento intermitente.	**31**	Circuito abierto (eléctrico).
15	Funcionamiento irregular.	**32**	Fugas (eléctricas).
16	Indicación errónea.	**33**	Otras condiciones excepcionales.
17	Flujo restringido.		-

Tabla 9.9: Modos de fallo genéricos

- **Análisis funcional (FA – Functional analysis)**

Teniendo en cuenta la relación que existe entre estructura y funcionamiento, se puede plantear la identificación de cómo cada uno de los elementos contribuyen a su funcionamiento, y la explicación de la función y los principios de funcionamiento de cada elemento y cómo contribuye cada uno de ellos al conjunto.

Realizaremos el análisis funcional con la construcción del árbol de funciones formado por las funciones elementales necesarias para obtener una imagen precisa de la arquitectura de funciones del producto. Se construye siguiendo la lógica de causa-efecto, desglosando cada función productiva en el siguiente nivel para alcanzar el propósito clave del árbol.

El diagrama funcional de nuestro sistema es el siguiente:

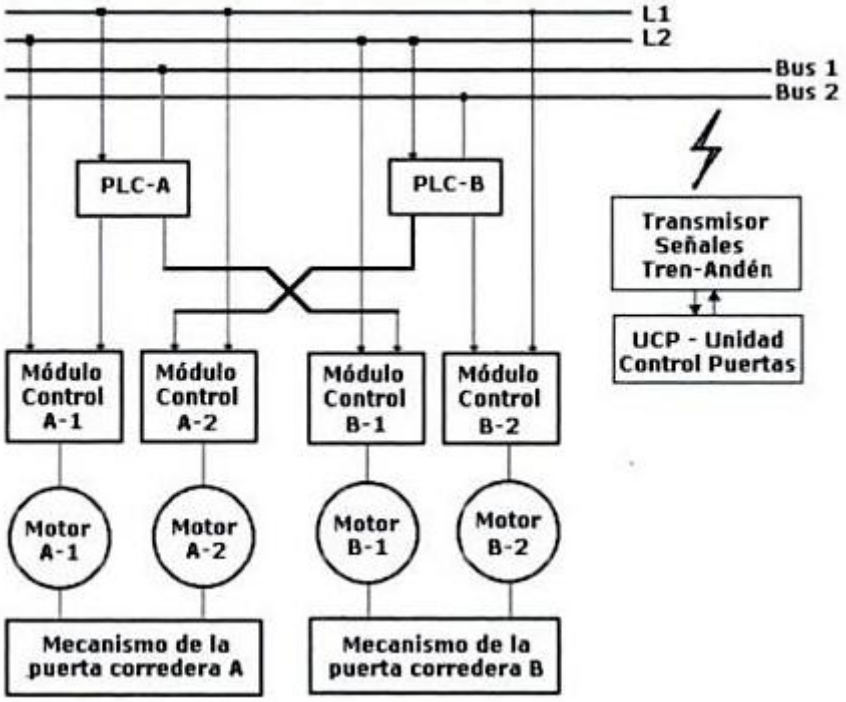

Figura 9.2: Diagrama funcional del sistema

- **Análisis preliminar de riesgos (PHA – Preliminary Hazard Analysis)**

El análisis preliminar de riesgos, PHA, sirve para clasificar cada componente RAM según la severidad del fallo.

El análisis PHA es utilizado únicamente en la fase de desarrollo de las instalaciones y para casos en los que no existen experiencias anteriores, sea del proceso o del tipo de instalación.

Selecciona los productos peligrosos existentes y los resultados incluyen recomendaciones para reducir o eliminar estos peligros, siempre de forma cualitativa. Requiere relativamente poca inversión en su realización.

Una de las aplicaciones típica de la tecnología RAMS es en ferrocarriles donde se utiliza la norma EN 50126. En la *tabla 9.10* se definen las categorías de riesgo de RAMS.

Frecuencia	I. Catastrófico	II. Crítico	III. Marginal	IV. Insignificante
A. Frecuente	1. Inaceptable	1. Inaceptable	1. Inaceptable	2. Indeseable
B. Probable	1. Inaceptable	1. Inaceptable	2. Indeseable	3. Tolerable
C. Ocasional	1. Inaceptable	2. Indeseable	3. Tolerable	3. Tolerable
D. Remota	2. Indeseable	3. Tolerable	3. Tolerable	4. Despreciable
E. Improbable	3. Tolerable	3. Tolerable	4. Despreciable	4. Despreciable

Tabla 9.10: Categoría, frecuencia y aceptabilidad del riesgo

El significado de los términos de la *tabla 9.10* se encuetra en las *tablas 9.11 a 9.13*.

Categoría riesgo	Descripción
I. Catastrófico	Muertes y daños materiales y medioambientales muy importantes.
II. Crítico	Lesiones graves a personas y daños materiales y medioambientales importantes.
III. Marginal	Lesiones leves a personas y daños materiales y medioambientales menores.
IV. Insignificante	Sin lesiones a personas ni daños materiales ni medioambientales.

Tabla 9.11: Categoría del riesgo

Frecuencia riesgo	Descripción
A. Frecuente	Aparece de forma continuada.
B. Probable	Aparece con frecuencia.
C. Ocasional	Es de esperar que aparezca de cuando en cuando.
D. Remota	Probabilidad razonable que aparezca en alguna ocasión.
E. Improbable	Es posible que aparezca de forma excepcional.

Tabla 9.12: Frecuencia del riesgo

Nivel de aceptación del riesgo	Descripción
1. Inaceptable	Debe eliminarse
2. Indeseable	Solo es aceptado si no es posible la reducción del riesgo y con la aprobación de la Autoridad competente.
3. Tolerable	Aceptable con el control adecuado y con la aceptación de la Autoridad competente.
4. Despreciable	Sin necesidad de aprobación de la Autoridad competente.

Tabla 9.13: Nivel de aceptación del riesgo

- **Análisis preliminar de disponibilidad (PAA – Preliminary Availability Analysis)**

La disponibilidad es la probabilidad de un sistema de estar en condiciones de funcionamiento en el tiempo t. El sistema no debe haber tenido fallos o bien, en caso de haberlos sufrido, debe haber sido reparado en un tiempo menor que el máximo permitido para su mantenimiento.

De este modo, si se considera un tiempo muy largo para el sistema, se tiene la llamada disponibilidad en régimen permanente, D(∞).

$$D_{\infty} = \frac{Tiempo\ total\ en\ condiciones\ de\ servicio}{Tiempo\ total\ del\ intervalo\ estudiado(condiciones\ de\ servicio + tiempo\ de\ paro)}$$

$$D_\infty = \frac{K \cdot MTBF}{K \cdot (MTBF + MTTR)} = \frac{\mu}{\mu + \lambda} = \frac{1}{1 + \frac{\lambda}{\mu}} \qquad (9.1)$$

donde:

MTBF = Tiempo medio entre fallos =1/λ.

MTTR = Tiempo medio de reparación = 1/μ.

K = Número de ciclos-reparación.

λ = Tasa de fallos (fallos/hora)

μ = Tasa de reparación (reparaciones/hora)

Nº.	Descripción	Ud	Función	λ (Fallos/h) · 10E6	μ - Operaciones de mantenimiento/h	D(∞) =1/(1+λ/μ)
1	**ARMAZÓN**	1				
1.1	Perfil principal y caucho rodadura	1	Guía y soporte carros y tope ruedas	0,0007	12	1,000000000
2	**MOTORIZACIÓN**	1				
2.1	Correa	1	Transmis. movim. a las hojas	15,4500	15	0,999998970
2.2	Codificador motor	1	Posición eje motor	1,0000	10	0,999999900
2.3	Grupo electrónico	1	Control sistema	12,7000	15	0,999999153
2.4	Motor completo	1	Movimiento y potencia a correa	1,0000	10	0,999999900
2.5	Cable alimentación	1	Energía al sistema	0,2200	30	0,999999993
3	**HOJA DER., IZQ.**	1				
3.1	Poleas de traslación	7	Movilización carro sobre guías	9,6300	2	0,999995185
3.2	Tope caucho	1	Rotación chapa	5,5000	5	0,999998900
3.3	Chapa leva de accionamiento	1	Accionamiento microrruptor	2,6700	20	0,999999867
4	**GRUPO PLC**	1	SCHNEIDER o similar	1,8300	15	0,999999878
5	**CHAPA CENTRAL**	1				
5.1	Chapa central	1	Soporte y centrado del microrruptor	2,6700	15	0,999999822
5.2	Tope de caucho	2	Tope movim. carros izq. y der.	5,9000	5	0,999998820
5.3	Microrruptor	4	Sensor contacto cierre y apertura puertas	0,3000	15	0,999999980
5.4	Enclavamiento mecánico	2	Enclavam. Cierre puertas por movim. Gatillo	15,0000	120	0,999999875

Tabla 9.14: Análisis preliminar de disponibilidad (PAA)

- Análisis previo de modos de fallo y de sus efectos FMECA (Failure Mode Effect and Critical Analysis).

El FMEA puede ampliarse incluyendo la probabilidad de cada modo de fallo y priorizando sus acciones correctivas, método que recibe el nombre de FMECA (Failure Modes, Effects and Criticality Analysis).

Para ello se calcula el llamado Número de Riesgo Prioritario (RPN – Risk Priority Number), que multiplica tres parámetros Severidad (S), Ocurrencia (O) y Detección (D) a los que se ha dado un valor numérico de 1 a 10 o de 1 a 5.

$$RPN = S \cdot O \cdot D \qquad (9.2)$$

donde:

S = Grado de severidad con escala 1 a 10 (o 1 a 5) en la que:
1 = el usuario no se ha enterado del fallo.
10 = existe un peligro grave o no se cumplen los reglamentos de seguridad.
O = Factor de ocurrencia del fallo con escala 1 a 10 (o 1 a 5), en el que:
1 = 1 fallo/100.000 y 10 = 1 fallo/10
D = Factor de detectabilidad, con escala 1 a 10 (o 1 a 5) en el que:
1 = se encuentra siempre el fallo.
10 = el fallo no es detectado por el usuario.

El valor de RPN obtenido se compara con los valores de otros Números de Riesgo Prioritario lo que permite determinar las áreas que se deben considerar para mejorar el sistema.

Nº.	Descripción	Ud.	Función	Modos de fallo		Causas de fallo	Consecuencias del fallo		Detección del fallo
				Generales	Genéricos		Efecto local	Efecto final	
1	**ARMAZÓN**	1	-	-	1	-	-	-	-
1.1	Perfil principal y caucho rodadura	1	Guía y soporte carros y tope ruedas	4	1	Defecto fabricación	Bloqueo puerta	Puerta inoperativa	Micros
2	**MOTORIZACIÓN**	1	-	-	-	-	-	-	-
2.1	Correa	1	Transmis. movim. a las hojas	4	1	Defecto fabricación	Puertas móviles	Puerta inoperativa	Micros
2.2	Codificador motor	1	Posición eje motor	4	18	Defecto fabricación	-	-	Mantenimiento
2.3	Grupo electrónico	1	Control sistema	4	30, 31, 32	Vibraciones - ajuste defectuoso	Motor inoperativo	-	Autómata
2.4	Motor completo	1	Movimiento y potencia a correa	4	18, 19, 20	Vibraciones - ajuste defectuoso	Motor inoperativo	-	Autómata
2.5	Cable alimentación	1	Energía al sistema	4	1, 32	Falla red	Puerta inoperativa	Puerta inoperativa	Micros
3	**HOJA DER., IZQ.**	1	-	-	-	-	-	-	-
3.1	Poleas de traslación	7	Movilización carro sobre guías	4	2	Desgaste	Puerta inoperativa	Puerta inoperativa	Micros
3.2	Tope caucho	1	Rotación chapa	4	1	Desgaste	-	-	Mantenimiento
3.3	Chapa leva de accionamiento	1	Accionamiento microrruptor	4	2, 4, 18	Desgaste, Vibraciones	Fallo cierre	Puerta inoperativa	Micros
4	**GRUPO PLC**	1	SCHNEIDER o similar	4	15, 18, 26, 27, 28, 29, 30, 31, 32	Avería	Motor no funciona	-	UCP
5	**CHAPA CENTRAL**	1	-	-	-	-	-	-	-
5.1	Chapa central	1	Soporte y centrado del microrruptor	4	1, 2, 3	Vibraciones	Micros no van	Puerta inoperativa	Micros
5.2	Tope de caucho	2	Tope movim. carros izq. y der.	4	1	Desgaste	Ruido	Desgaste enclavam.	Mantenimiento
5.3	Microrruptor	4	Sensor contacto cierre y apertura puertas	4	2, 5, 6, 7, 8, 21, 30, 31	Avería	PLC no recibe señal	-	PLC
5.4	Enclavamiento mecánico	2	Enclavam. Cierre puertas por movim. Gatillo	4	1, 2	Desgaste	Fallo micro	Micros inoperativos	PLC

Tabla 9.15: Análisis previo FMECA

Nº.	Severidad (S)	Ocurrencia (O)	Detección (D)	Criticidad (RPN=S·O·D)	Medidas correctoras	λ (fallos/hora)·10E6
	Índices (1 a 5)					
1						-
1.1	3	5	4	60	Calidad fabricación	0,0007
2						-
2.1	2	3	3	18	Manten. Preventivo	15,4500
2.2	4	4	3	48	Manten. Preventivo	1,0000
2.3	2	3	3	18	Sustitución	12,7000
2.4	3	4	3	36	Sustitución	1,0000
2.5	2	4	3	24	SAI	0,2200
3						-
3.1	2	5	3	30	Sustitución	9,6300
3.2	3	3	3	27	Sustitución	5,5000
3.3	2	4	3	24	Sustitución	2,6700
4	2	3	2	12	Sustitución	1,8300
5						-
5.1	2	5	3	30	Sustitución	2,6700
5.2	3	4	3	36	Sustit. ajuste	5,9000
5.3	3	5	3	45	Sustitución	0,3000
5.4	3	4	3	36	Sustitución	15,0000

Tabla 9.16: Análisis previo FMECA (cont.)

9.2.4 Etapa 3: Análisis por árbol de fallos (FTA) y Diagrama de bloques de fiabilidad (RBD)

- **Análisis por árbol de fallos FTA (Fault Tree Analysis) de los eventos.**

  Análisis explicado en el *Apartado 8*.

- **Análisis lógico.**

Para el análisis lógico se utilizan tres técnicas básicas: estudio, reducción booleana y determinación de cortes mínimos. La base del análisis lógico es la modelización. Una modelización correcta supone representar las funciones o

componentes de un sistema de forma que se establezcan sus interacciones, dependencias, causas inmediatas de resultados desfavorables, etc.

- **Análisis numérico.**

La finalidad del análisis numérico es proporcionar una evaluación cuantitativa de la probabilidad de que ocurra el suceso superior o un conjunto seleccionado de sucesos. También puede emplearse para apoyar y complementar el análisis lógico. Para realizar una evaluación numérica de un árbol de fallo se necesitan datos probabilísticos a nivel componente.

- **Ejemplo:**

Por no extendernos realizando el análisis por árbol de fallo para todos los posibles fallos de nuestro caso, haremos el estudio sólo para el fallo de Cierre de puertas con un pasajero atrapado.

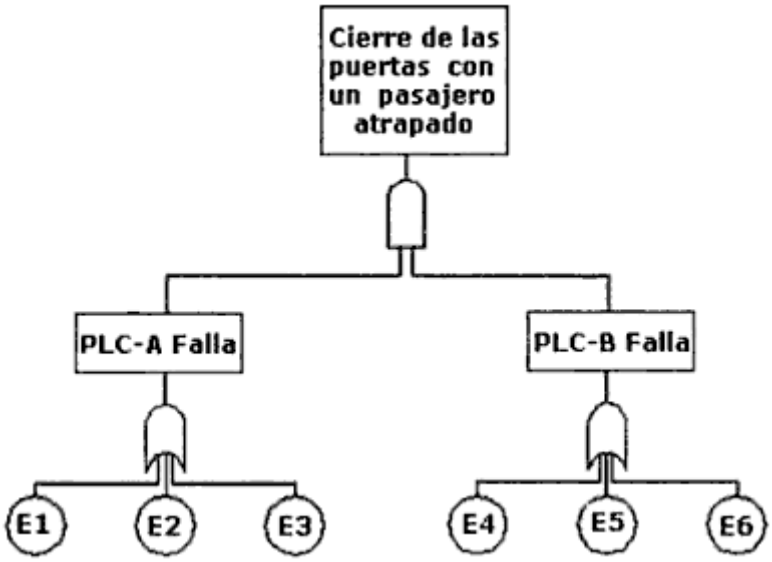

Figura 9.3: Árbol de fallos de Cierre de puertas con un pasajero atrapado

Los eventos básicos son:

E1: Fallo alimentación eléctrica L1.
E2: Fallo comunicación bus1.
E3: Fallo autómata PLC-A.
E4: Fallo comunicación bus2.
E5: Fallo autómata PLC-B.
E6: Fallo alimentación eléctrica L2.

Análisis lógico:

Evento Principal (TOP EVENT) = PLCA·PLCB = (E1+E2+E3)·(E4+E5+E6) = E1·E4+E1·E5+E1·E6+E2·E4+E2·E5+E2·E6+E3·E4+E3·E5+E3·E6

Análisis cuantitativo:

A = PLC-A falla = E1 + E2 + E3 - E1·E2 - E1·E3 - E2·E3 + E1·E2·E3

B = PLC-B falla = E4 + E5 + E6 - E4·E5 - E4·E6 - E5·E6 + E4·E5·E6

C = Cierre de puertas con un pasajero atrapado = A·B

Descripción Fallos	λ (Fallo/año)	λ (Fallo/hora)·10E6	Infiabilidad exponencial (en un año) (1-exp(-λt))	Fiabilidad exponencial (en un año) (exp(-λ·t))
E1: Fallo alimentación eléctrica L1	0,07008000	8,11	0,06768077	0,93231923
E2: Fallo comunicación bus1	0,03942000	4,56	0,03865314	0,96134686
E3: Fallo autómata PLC-A	0,01576800	1,83	0,01564434	0,98435566
E4: Fallo comunicación bus2	0,03942000	4,56	0,03865314	0,96134686
E5: Fallo autómata PLC-B	0,01576800	1,83	0,01564434	0,98435566
E6: Fallo alimentación eléctrica L2	0,07008000	8,11	0,06768077	0,93231923
A = PLC-A falla = E1 + E2 + E3 -E1·E2 - E1·E3 - E2·E3 + E1·E2·E3			0,11773957	0,99995907
B = PLC-B falla = E4 + E5 + E6 - E4·E5 - E4·E6 - E5·E6 + E4·E5·E6			0,11773957	0,99995907
C = Cierre de Puertas con un Pasajero Atrapado = A·B			0,01386261	0,99991815

Tabla 9.17: Análisis cuantitativo del árbol de fallo de cierre de puertas con un pasajero atrapado.

- **Diagrama de bloques de fiabilidad (RBD – Reliability Block Diagrams).**

El Digrama de bloques de fiabilidad se rige por la norma UNE-EN 61078:2006.

Un diagrama de bloques de fiabilidad es una representación gráfica del comportamiento de la fiabilidad de un sistema. Muestra las conexiones lógicas entre los componentes (funcionales) necesarios para el correcto funcionamiento del sistema.

La técnica de realización de modelos de diagramas de bloques de fiabilidad está pensada principalmente para sistemas no reparables y en los que no importa el orden en que se producen los fallos. En los sitemas en los que el orden de aparición de los fallos deba tenerse en cuenta, o en sistemas reparables es más conveniente el uso de otras técnicas como el anáisis de Markov. En este caso, el del análisis RAMS,

como se va a emplear combinado con otros métodos podremos utilizarlo aunque los sitemas sean reparables.

Una de las hipótesis en que se basa el RBD, es que los componentes sólo pueden encontrarse en dos estados: operativos o fallado. Otra hipótesis es que el fallo (o reparación) de cualquier bloque no debe afectar a la probabilidad de fallo (o reparación) de cualquier otro bloque en el sistema modelado.

Existen varios métodos para la evaluación cuantitativa de un RBD. Dependiendo del tipo de estructura pueden emplearse técnicas booleanas simples o análisis de corte y mínimo. Los cálculos pueden hacerse usando los métodos básicos de fiabilidad o disponibilidad de los componentes y métodos analíticos o simulación de Monte Carlo.

El primer paso es elegir una definición de éxito o fallo del sistema. Si hay más de una definición pueden requerirse diagramas de bloques de fiabilidad diferentes para cada una. El siguiente paso es dividir el sistema en bloques para reflejar su comportamiento lógico, de modo que cada bloque sea estadísticamente independiente de los otros y tan grande como sea posible. Además los bloque no deberías contener redundancias.

El siguiente paso es remitirse a la definición de éxito o fallo del sistema y construir un diagrama que conecte los bloques para formar un “camino de éxito”. Los distintos caminos de éxito, entre los puntos de entrada y salida del diagrama, atraviesan las combinaciones de bloques que es necesario que funcionen para que el sistema funcione.

En nuestro caso:

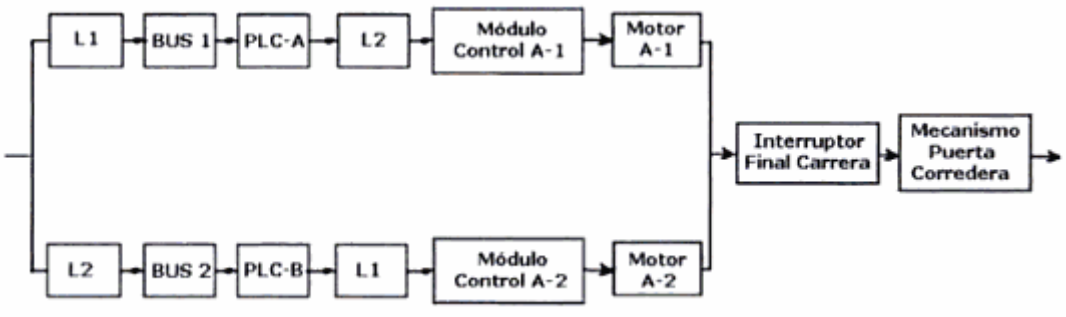

Figura 9.4: Diagrama de bloques de fiabilidad

La fiabilidad del sistema es:

R1 (Bloque superiores) = L1·BUS1·PLCA·L2·(Módulo Control A-1)·(Motor A-1)
R2 (Bloques inferiores) = L2·BUS2·PLCB·L1·(Módulo Control A-2)·(Motor A-2)
Rtotal = [1-(1-R1)·(1-R2)]·(Interruptor Final Carrera)·(Mecanismo Puerta Corredera)

Descripción Fallos	λ (Fallo/año)	λ (Fallo/hora)	Fiabilidad exponencial/hora (exp(-λ·t))
M1 - Motor A-1	0,00876000	0,00000101	0,99999899
M1 - Motor A-2	0,00876000	0,00000101	0,99999899
Módulo Control A-1	0,11388000	0,00001318	0,99998682
Módulo Control A-2	0,11388000	0,00001318	0,99998682
PLC-A	0,01576800	0,00000183	0,99999818
PLC-B	0,01576800	0,00000183	0,99999818
Mecanismo Puerta Corredera	0,02277600	0,00000264	0,99999736
Alimentación eléctrica L1	0,07008000	0,00000811	0,99999189
Alimentación eléctrica L2	0,07008000	0,00000811	0,99999189
Comunicación Bus1	0,03942000	0,00000456	0,99999544
Comunicación Bus2	0,03942000	0,00000456	0,99999544
Interruptor Final Carrera	0,68065200	0,00007878	0,99992122
R1 (Bloques superiores) = L1·Bus1·PLCA·L2·(Módulo Control A-1)·(Motor A-1)			0,9999631965
R2 (Bloques inferiores) = L2·Bus2·PLCB·L1·(Módulo Control A-2)·(Motor A-2)			0,9999631965
Rtotal = [1-(1-R1)·(1-R2)]·(Interruptor Final Carrera)·(Mecanismo Puerta Corredera)			0,9999999986
1/hora del sistema = -Ln(Rtotal)/1			1,35450E-09
1/hora/andén del sistema = 2·(-Ln(Rtotal)/1) (Sólo 1 vagón de 2 puertas en el andén)			2,70899E-09

Tabla 9.18: Fiabilidad del sistema (un vagón con dos puertas)

9.2.5 Etapa 4: Mantenimiento preventivo

El mantenimiento preventivo mejora la fiabilidad del equipo y además tiene la ventaja de poderse programar, es decir, de ejecutar en el momento más favorable.

En este apartado confirmaremos el tiempo medio de reparación (MTTR) con indicación del tiempo de recambio de componentes y del número de operarios necesario. Estudiaremos también la calidad del servicio (QoS). El objetivo de calidad del servicio está basado en el tiempo medio entre fallos que afecten al servicio (MTBFs), el tiempo medio para restaurar el servicio (MTTRs) y una disponibilidad determinada.

Comprobaremos si se cumplen los objetivos de disponibilidad y fiabilidad establecidos en la *Etapa 1*, teniendo en cuenta las redundancias implantadas en los subsistemas y todos los criterios de seguridad adoptados.

En el caso de nuestro ejemplo, el mantenimiento preventivo viene fijado por el tiempo y número de ciclos. El módulo de control cuantifica los ciclos de apertura y cierre realizados. No se contempla el tiempo de desplazamiento de los operarios y se supone que los operarios, las herramientas y las piezas de recambio están a pie de andén.

OPERACIONES POR REALIZAR	PERIODICIDAD		TIEMPOS DE INTERVENCIÓN (minutos)	Nº. OPERARIOS MANTENIMIENTO	CALIDAD DEL SERVICIO (QoS)	
	CICLOS	MESES			MTBF (horas)	MTTR (min)
Mecanismo Apertura/Cierre	-	6	2	1	500.000	2
Limpieza del perfil de rodamiento	-	6	5	1	181.818	5
Comprobación y ajuste de las ruedas	-	6	8	1	103.842	8
Comprobación topes elásticos de los carros	1.000.000	-	12	1	169.491	12
Cambiar piñones	2.500.000	-	25	1	103.842	25
Cambiar correa	2.500.000	-	4	1	64.725	4
Cambiar ruedas	2.500.000	-	30	1	275.482	30
Cambiar perfil de rodamiento	5.000.000	-	20	1	181.818	20

Tabla 9.19: Mantenimiento preventivo

OPERACIONES POR REALIZAR	OBJETIVO DISPONIBILIDAD DE SERVICIO 99,99%	OBJETIVO FIABILIDAD SISTEMA 99,992%			RECOMENDACIONES
	Disponibilidad	λ fallos/h · 10E6	Redundancía (Sí/No)	Fiabilidad	
Mecanismo Apertura/Cierre	0,999999933	2,0	Sí	0,999998000000	-
Limpieza del perfil de rodamiento	0,999999542	5,5	No	0,999994499995	Aumentar frec. limpieza.
Comprobación y ajuste de las ruedas	0,999998716	9,6	No	0,999990369985	Aumentar frec. ajuste.
Comprobación topes elásticos de los carros	0,999998820	5,9	No	0,999994099982	Aumentar frec. cambios.
Cambiar piñones	0,999995988	9,6	No	0,999990369985	-
Cambiar correa	0,999998970	15,4	No	0,999984550019	Aumentar frec. cambios.
Cambiar ruedas	0,999998185	3,6	No	0,999996369999	Aumentar frec. cambios.
Cambiar perfil de rodamiento	0,999998167	5,5	No	0,999994499995	Aumentar frec. cambios.

Tabla 9.20: Mantenimiento preventivo (cont.)

9.2.6 Etapa 5: Unidades reemplazables

- **Listado de la probabilidad de fallo de los componentes de los subsistemas que puedan reemplazarse y de su tiempo medio de reparación (MTTR)**

El Tiempo medio de reparación, MTTR, consta de: tiempo de diagnóstico + tiempo de recambio y ajuste + tiempo de puesta en servicio.

Ítem	DESCRIPCIÓN	UDS	FUNCIÓN	MTTR (min)	λ (fallos/h)· 10E6	MTTR (minutos)		
						T. DIAGNÓSTICO	T. RECAMBIO Y AJUSTE	T. PUESTA EN SERVICIO
1	Unidad de control de puertas.	2	Ubicada en el andén. Controla el sistema tren-andén.	4	10,0	-	-	-
2	Módulo control.	1	Controla la puerta corredera.	4	1,8	-	-	-
3	Control señales sistema.	1	Grupo electrónico control motor puerta corredera.	4	13,3	-	-	-
4	Motor.	2	Generación del movimiento y de la potencia a la correa.	6	1,0	-	-	-
5	Transmisor señales tren-andén.	1	Intercambia información entre la cabecera del tren y el andén.	5	2,0	-	-	-

Tabla 9.21: MTTR Unidades desmontables

- **MTBF. Disponibilidad del servicio (MTBSF). Conclusiones, recomendaciones, acciones correctoras y redundancias implementadas en el diseño. Propuesta para comprobar, verificar empíricamente y certificar los valores indicados.**

Ítem	DESCRIPCIÓN	CANTIDAD	FUNCIÓN	MTBF (horas)	MTBSF - DISPONIBILIDAD DE SERVICIO (andén) (horas)	HIPÓTESIS DE PARTIDA Y BASES DE DATOS DE CÁLCULO
1	Unidad de control de puertas.	2	Ubicada en andén. Controla sistema tren-andén.	100.000	150.000	Equipo no redundante.
2	Módulo control.	1	Controla la puerta corredera.	545.161	1.090.322	Equipo redundante.
3	Control señales del sistema.	1	Grupo electrónico control motor puerta corredera.	74.880	149.760	Equipo redundante.
4	Motor.	2	Generación del movimiento y de la potencia a la correa.	1.000.000	2.000.000	Equipo redundante.
5	Transmisor señales tren-andén.	1	Intercambia información entre cabecera tren y andén.	300.000	350.000	Equipo redundante.

Tabla 9.22: MTBF, MTBSF, Hipótesis

Ítem	DISEÑO				PROPUESTA DE COMPROBACIÓN, VERIFICACIÓN EMPÍRICA Y CERTIFICACIÓN DE LOS VALORES OFERTADOS	
	CONCLU-SIONES	RECOMEN-DACIONES	ACCIONES CORRECTORAS	REDUN-DANCIAS	PROTOTIPOS	INSTALACIÓN TERMINADA PENDIENTE DEL PERÍODO DE GARANTÍA
1	Podría duplicarse.	Duplicar.	Cierre manual.	Sí.	Certificación ISO 9000-2000.	Ensayos en laboratorio para obtener la certificación.
2	Sistema suficiente.	Mto. preventivo a modificar s/experiencia.	El otro autómata (PLC) toma el control.	Sí.	Árbol fallos para puntos débiles. Análisis FMECA para fallos que interrumpen servicio.	Ensayos en laboratorio para obtener la certificación.
3	Sistema suficiente.	Mto. preventivo a modificar s/experiencia.	La electrónica duplicada toma el control.	Sí.	Árbol fallos para puntos débiles. Análisis FMECA para fallos que interrumpen servicio.	Ensayos en laboratorio para obtener la certificación.
4	Sistema suficiente.	Mto. preventivo a modificar s/experiencia.	El otro motor toma el control.	Sí.	Árbol fallos para puntos débiles. Análisis FMECA para fallos que interrumpen servicio.	Ensayos en laboratorio para obtener la certificación.
5	Sistema suficiente.	Acortar períodos mto. preventivo.	Control manual.	Sí.	Certificación ISO 9000-2000.	Ensayos en laboratorio para obtener la certificación.

Tabla 9.23: Conclusiones y Propuesta por andén

- **Coste de los componentes desmontables que se han de sustituir, el coste de su reparación y el número de reparaciones posible.**

Para un posterior análisis económico del sistema, se debería indicar los costes que conllevan la sustitución y/o reparación de los componentes.

9.2.7 **Etapa 6: Análisis de riesgos.**

Los sistemas industriales complejos interaccionan en formas complicadas y a veces imprevistas. En un gran sistema es a veces irrealizable ensayar cada componente y mucho menos todas las combinaciones posibles. Las técnicas de

análisis de riesgos pueden ser útiles para analizar las interacciones potenciales entre las partes del sistema.

El análisis de operatibilidad examina toda posible desviación en el funcionamiento y el comportamiento de un proceso. Su objetivo es prever las consecuencias de las desviaciones en la operación normal del proceso. Es de tipo cualitativo.

Pertenecen al método inductivo los análisis de FMEA/FMECA, HAZOP, Markov, Árbol de Fallos y el Diagrama de bloques de fiabilidad.

El estudio que nos interesa para esta etapa es el **método HAZOP** (HAZard and OPerability). Su objetivo es la búsqueda de relaciones entre las causas y sus consecuencias.

Su realización engloba la colaboración de expertos en diferentes áreas de conocimiento que aportan su experiencia y así identifican más problemas que si lo hicieran por separado.

El método de *HAZOP modificado* es una ampliación del proceso seguido en el HAZOP. Es un método cualitativo en el que un equipo de expertos le asigna un valor, el *SIL* (Safety Integrity Level = Nivel de Seguridad), para evaluar las consecuencias potenciales de un evento del proceso. El *Ciclo de Vida* de un instrumento representa todas las fases del dispositivo, el diseño, la instalación, la operación, el mantenimiento y la comprobación. Dentro del ciclo de vida, el *SIL* especifica el *Nivel de Integridad de la Seguridad* que define, en función del posible impacto de un fallo sobre personas y bienes y su probabilidad, el nivel de seguridad requerido del sistema y , por tanto, de todos sus componentes.

Cuanto más alto es el *SIL*, más baja es la probabilidad de que el sistema falle y, por lo tanto, mayor ha de ser el nivel de protección y a la inversa.

No existen reglamentaciones que asignen un nivel *SIL* a un proceso en particular, por lo que la asignación es una decisión corporativa basada en una filosofía de gestión de riesgos y de su tolerancia.

El *SIL* está relacionado con la probabilidad media de fallo a la demanda por año (PFDavg).

Existe una relación entre la seguridad y la disponibilidad. El sistema de seguridad no debe parar el proceso ante fallos internos (paradas falsas) pues afectaría

la disponibilidad, y la probabilidad de una parada del proceso no deseada debe ser baja para no afectar la disponibilidad, lo cual repercutiría en la economía del proceso.

La relación entre el Nivel de Integridad de la Seguridad (SIL) y la probabilidad de fallo a la demanda (PFD) puede verse en la siguiente tabla:

SIL	PFD Probabilidad de fallo a la demanda	Disponibilidad (1-PFD)	1/PFD tiempo medio entre fallos	Impacto sobre personal
4	10^{-5} a 10^{-4}	> 99,99%	100.000 a 10.000	Impacto catastrófico
3	10^{-4} a 10^{-3}	99,90 - 99,99%	10.000 a 1.000	Protección al personal
2	10^{-3} a 10^{-2}	99,00 - 99,90%	1.000 a 100	Protección importante
1	10^{-2} a 10^{-1}	90,00 - 99,00%	100 a 10	Protección pequeña

Tabla 9.24: Correlación entre SIL y PFD

El valor cualitativo del *SIL* puede expresarse como una consecuencia de los fallos en el sistema de seguridad (SIS), en términos de daños a personas e instalaciones.

SIL	Consecuencias	Interpretación
4	Impacto catastrófico (catastrófico).	Intolerable. Muerte de una o más personas. Pérdidas de producción y de capital mayores de 10 millones €.
3	Impacto en personas y en la comunidad (crítico).	Indeseable. Muerte de una persona y lesiones múltiples a la comunidad. Pérdidas de producción y de capital entre 1 y 10 millones €. Sólo debe aceptarse si la reducción del riesgo es impracticable.
2	Daños importantes en la producción y en la propiedad. Posibles lesiones a personas que requieren hospitalización (marginal).	Tolerable con el apoyo responsable del Comité de Seguridad. Pérdidas de producción y de capital entre 50.000 y 1 millón de €.
1	Daños poco importantes en personas y en instalaciones (despreciable).	Tolerable con el respaldo del Comité de Seguridad a las revisiones normales de los proyectos. Lesiones de escasa gravedad. Sin daños en el medio ambiente. Pérdidas de producción menores de 50.000 €.

Tabla 9.25: Valor cualitativo del SIL

La *matriz de riesgo* es una herramienta para la evaluación cualitativa del riesgo. Proporciona una correlación entre la severidad de dicho riesgo y su frecuencia.

Severidad	**Catastrófico**	SIL3	SIL 3	-	-
	Crítico	SIL2	SIL 2	SIL 3	SIL 3
	Marginal	SIL1	SIL 1	SIL 2	SIL 2
	Despreciable	No Riesgo	No Riesgo	SIL 1	SIL 1
		Raro	**Ocasional**	**Probable**	**Frecuente**
		Frecuencias			

Tabla 9.26: Ejemplo de matriz de riesgo

El riesgo cuantitativo es la valoración realizada con índices de fallos y, en algunos casos, se evalúa el impacto potencial. Se utilizan técnicas de determinación cuantitativa de la probabilidad de fallo a la demanda por año (PFDavg) (ecuaciones simplificadas o el análisis por árbol de fallos o el análisis de Markov). En el caso de que el *SIL* calculado sea inferior o igual al *SIL* objetivo, es necesario aplicar al proceso, o bien una mejor tecnología, o bien una mayor redundancia.

El riesgo para el usuario es que si sobredimensiona el sistema de seguridad le resultará caro y, al contrario, si el diseño es insuficiente, se expone a un riesgo excesivo y a la producción de incidentes en el proceso.

Las ventajas que presenta para el usuario la gestión correcta de la seguridad son:

- Cumple los estándares de seguridad.
- Disponibilidad óptima de la planta.
- Aumento de la productividad.
- Mejor mantenimiento.
- Mejor seguridad del proceso.
- Aumento de la vida útil de la planta.

Análisis de riesgos de nuestro ejemplo:

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	MODO DE FALLO (Cómo se detecta)	DETECCIÓN FALLO Y MÉTODOS PROTECCIÓN	EFECTOS DEL FALLOS (Operación, Función o Estado del sistema)
1	Unidad de control de puertas.	2	Ubicada en el andén. Controla el sistema tren-andén.	Fallo comunicación, alimentación, y sus componentes.	Alarma. Verificación de la comunicación y alimentación. Señal de paro del sistema.	Mal funcionamiento puertas. Sistema parado.
2	Módulo control.	1	Controla la puerta corredera.	Puertas no funcionan. Descarrilamiento puertas y avería en mecanismo.	Alarma. Inspección física. Señal de paro.	Paro del sistema. Puertas descarriladas.
3	Control señales sistema.	1	Grupo electrónico control motor puerta corredera.	Fallo comunicación. Fallo alimentación eléctrica.	Alarma.	Paro del sistema. Puertas no funcionan.
4	Motor.	2	Generación del movimiento y de la potencia a la correa.	Fallo en circuitos, en comunicación con PLC y en alimentación.	Alarma.	Sobrecarga motor y daños en el mecanismo de deslizamiento.
5	Transmisor señales tren-andén.	1	Intercambia información entre la cabecera del tren y el andén.	Fallo dispositivos transmisión y recepción señales. Fallo en comunicación.	Alarma. Descoordinación de las puertas respecto al tren.	Parada del sistema.

Tabla 9.27: Análisis de riesgos

Nº.	Índice Severidad (S) (1 a 5)	Índice Ocurrencia (O) (1 a 5)	Índice Detección (D) (1 a 5)	Índice Criticidad (RPN=S·O·D)	SIL (Safety Integrity Level)
1	2	4	2	16	4
2	2	3	2	12	4
3	3	4	2	24	3
4	3	4	2	24	3
5	2	3	2	12	3

Tabla 9.28: Análisis de riesgos (cont.)

Nº.	PROBABILIDAD FALLOS A LA DEMANDA (PFD)	DISPONIBILIDAD (1 - PFD)	(1/PFD)	RIESGO EN SEGURIDAD PERSONAS	MEDIDAS CORRECTIVAS O PREVENTIVAS PARA REDUCIR EL PELIGRO
1	0,0001	0,9999	10.000	4	Sistema auxiliar en paralelo o alarma visual o menaje al pasajero.
2	0,0001	0,9999	10.000	3	Alarma visual o mensaje al pasajero.
3	0,001	0,999	1.000	4	Sistema auxiliar en paralelo o alarma visual o menaje al pasajero.
4	0,001	0,999	1.000	4	Sistema auxiliar en paralelo o alarma visual o menaje al pasajero.
5	0,001	0,999	1.000	4	Sistema auxiliar en paralelo o alarma visual o menaje al pasajero.

Tabla 9.29: Análisis de riesgos (cont.2)

9.2.8 **Etapa 7: Estudio previo de RAMS en detalle**

En las etapas anteriores se han estimado los datos y los diagramas de forma preliminar. En esta etapa se analizan los mismos en detalle:

- Tiempo medio entre fallos MTBF (Mean Time Between Failures).
- Diagramas de representación – Análisis de árbol de fallos FTA (Failure Tree Analysis) + esquemas lógicos + diagramas de estado + diagramas de eventos, etc.
- Análisis de modos de fallos, efectos y criticidad de los subsistemas (FMECA).
- Disponibilidad de los subsistemas.
- Análisis de la fiabilidad del software.
- Tiempo medio de reparación (MTTR) y tasa de reparación.
- Análisis del mantenimiento preventivo (periodicidad, tiempo de respuesta, personal material, coste del material, etc.).
- Planes de contingencia y aislamiento de fallos y de averías.
- Análisis de riesgos según la norma aplicable.
- Clasificación de cada riesgo.
- Efecto de cada situación de riesgo en la seguridad del personal.
- Medidas correctivas y preventivas para reducir el riesgo.
- Estimación de la clasificación del riesgo después de aplicar la medida correctiva.

- Nivel de aceptación del riesgo.
- Demostración de la fiabilidad, disponibilidad, mantenibilidad y seguridad.
- Ensayos para realizar y su valoración.
- Inventario de datos de la instalación para realizar los programas de predicción y demostración de RAMS.

Dada la simplificación de nuestro caso, supondremos que no habrá gran diferencia con los valores indicados en las etapas anteriores.

- **Estudio previo de RAMS**

RAMS representa un indicador, tanto cualitativo como cuantitativo, del grado de confianza que ofrece un sistema para comportarse de acuerdo a la funcionalidad especificada, de forma segura y con una alta disponibilidad.

Con los datos iniciales y los resultados obtenidos en las etapas anteriores completamos una tabla en la que se reúne toda la información importante del análisis RAMS.

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	MODO DE FALLO (Cómo se detecta)	DETECCIÓN FALLO Y MÉTODOS PROTECCIÓN	EFECTOS DEL FALLOS (Operación, Función o Estado del sistema)
1	Unidad de control de puertas.	2	Ubicada en el andén. Controla el sistema tren-andén.	Fallo comunicación, alimentación, y sus componentes.	Alarma. Verificación de la comunicación y alimentación. Señal de paro del sistema.	Mal funcionamiento puertas. Sistema parado.
2	Módulo control.	1	Controla la puerta corredera.	Puertas no funcionan. Descarrilamiento puertas y avería en mecanismo.	Alarma. Inspección física. Señal de paro.	Paro del sistema. Puertas descarriladas.
3	Control señales sistema.	1	Grupo electrónico control motor puerta corredera.	Fallo comunicación. Fallo alimentación eléctrica.	Alarma.	Paro del sistema. Puertas no funcionan.
4	Motor.	2	Generación del movimiento y de la potencia a la correa.	Fallo en circuitos, en comunicación con PLC y en alimentación.	Alarma.	Sobrecarga motor y daños en el mecanismo de deslizamiento.
5	Transmisor señales tren-andén.	1	Intercambia información entre la cabecera del tren y el andén.	Fallo dispositivos transmisión y recepción señales. Fallo en comunicación.	Alarma. Descoordinación de las puertas respecto al tren.	Parada del sistema.

Tabla 9.30: Estudio previo de RAMS

Nº.	Índice Severidad (S) (1 a 5)	Índice Ocurrencia (O) (1 a 5)	Índice Detección (D) (1 a 5)	Índice Criticidad (RPN=S·O·D)	SIL (Safety Integrity Level)
1	2	4	2	16	4
2	2	3	2	12	4
3	3	4	2	24	3
4	3	4	2	24	3
5	2	3	2	12	3

Tabla 9.31: Estudio previo de RAMS (cont.)

Nº.	λ (Fallo/h) ·10E6	λ (Fallo/año)	FIABILIDAD (1-λ)	MTBF (1/λ)	MTTR (min)	μ (Nº reparac./h) = 1/MTTR	DISPONIBILIDAD μ/(μ+λ)
1	10,00	0,08640	0,9999900	100.000	4	15	0,9999993
2	1,80	0,01555	0,9999982	555.556	4	15	0,9999999
3	13,30	0,11491	0,9999867	75.188	4	15	0,9999991
4	1,00	0,00864	0,9999990	1.000.000	6	10	0,9999999
5	2,00	0,01728	0,9999980	500.000	5	12	0,9999998

Tabla 9.32: Estudio previo de RAMS (cont.2)

Nº.	SOFTWARE λ	FIABILIDAD DEL SOFTWARE	MANTENIMIETO PREVENTIVO				
			Periodicidad (horas)	Tiempo respuesta (horas)	Personal	Material	Coste material
1	0,0000425	0,9999575	50.000	0,07	1	-	-
2	-	-	187.000	133	1	-	-
3	-	-	39.440	0,067	1	-	-
4	-	-	500.000	0,1	1	-	-
5	-	-	45.045	0,067	1	-	-

Tabla 9.33: Estudio previo de RAMS (cont.3)

Nº.	MANTENIMIENTO CORRECTIVO						PLANES CONTINGENCIA	AISLAMIENTO, FALLOS Y AVERÍAS
	λ (Fallo/hora) ·10E6	MTBF (horas)	Tiempo respuesta (horas)	Personal	Material	Coste material		
1	10,00	100.000	0,084	1	-	-	Equipo redundante de reserva.	Aislar en bypass componentes (sist. alimentac. y comunic.)
2	1,80	555.556	0,16	1	-	-	Equipo redundante de reserva.	Aislar en bypass componentes (sist. alimentac. y comunic.)
3	13,30	75.188	0,08	1	-	-	Equipo redundante de reserva.	Aislar en bypass componentes (sist. alimentac. y comunic.)
4	1,00	1.000.000	0,12	1	-	-	Equipo redundante de reserva.	Aislar en bypass componentes (sist. alimentac. y comunic.)
5	2,00	500.000	0,08	1	-	-	Equipo redundante de reserva.	Aislar en bypass componentes (sist. alimentac. y comunic.)

Tabla 9.34: Estudio previo de RAMS (cont.4)

9.2.9 Etapa 8: Requisitos mínimos de fiabilidad, mantenimiento y disponibilidad.

Esta etapa consiste en definir los siguientes aspectos:

- Requisitos mínimos RAM de los componentes integrados y asociados a los subsistemas, especificando MTBF, Tasa de fallos (λ), análisis cualitativo, análisis cuantitativo en árboles de fallos.
- Plan de seguimiento de la fiabilidad para verificar la fiabilidad del sistema durante su vida útil.

  El plan de seguimiento consiste en definir los métodos de supervisión del sistema, como instrumentos de monitorización, para asegurar el buen funcionamiento de éste. El plan de seguimiento se puede ir adecuando a las nuevas circunstancias y situaciones que se produzcan.

- Mantenibilidad con los parámetros MTTR, MDT (Tiempo medio de inmovilización), TCBF (Tiempo acumulado de buen funcionamiento), TCIR

(Tiempo acumulado de paralización de la instalación debido al mantenimiento correctivo), Número de intervenciones de mantenimiento con paralización del servicio.

- Disponibilidad con los tipos de fallos, su incidencia en el servicio, los retardos provocados en el sistema, el tiempo para la detección y reparación de los fallos, las medidas provisionales que se deben adoptar para disminuir la degradación del servicio y la información que se considere relevante.

9.2.10 Etapa 9: Características de los componentes.

Debido al carácter limitado de nuestro estudio ejemplo no se detallan los requisitos mínimos de los componentes integrados y sólo de los componentes significativos.

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	FACTORES DE CONTRIBUCIÓN A LA DISPONIBILIDAD DEL SISTEMA												CONTRIBUCIÓN DE CADA ELEMENTO	
				COMPLEJIDAD		ESTADO		TIEMPO DE FUNCIONA-MIENTO		CONDICIONES DE CONTORNO		FACILIDAD DE REPARACIÓN		REDUN-DANCIA		Peso	Ponderación sobre el total
				0,05		0,1		0,2		0,05		0,15		0,45		1	
1	**ARMAZÓN**	1	-														
1.1	Perfil principal y caucho rodadura	1	Guía y soporte carros y tope ruedas	3	0,15	3	0,3	1	0,2	3	0,15	2	0,30	1	0,45	1,55	6,90%
2	**MOTORIZA-CIÓN**	1	-														
2.1	Correa	1	Transmis. movim. a las hojas	3	0,15	3	0,3	1	0,2	3	0,15	2	0,30	1	0,45	1,55	6,90%
2.2	Codificador motor	1	Posición eje motor	1	0,05	3	0,3	1	0,2	1	0,05	1	0,15	2	0,90	1,65	7,35%
2.3	Grupo electrónico	1	Control sistema	1	0,05	3	0,3	2	0,4	3	0,15	1	0,15	2	0,90	1,95	8,69%
2.4	Motor completo	1	Movimiento y potencia a correa	1	0,05	3	0,3	1	0,2	1	0,05	1	0,15	2	0,90	1,65	7,35%
2.5	Cable alimentación	1	Energía al sistema	2	0,10	3	0,3	1	0,2	2	0,10	2	0,30	2	0,90	1,90	8,46%
3	**HOJA DER., IZQ.**	1	-														
3.1	Poleas de traslación	7	Movilización carro sobre guías	2	0,10	3	0,3	1	0,2	1	0,05	1	0,15	1	0,45	1,25	5,57%
3.2	Tope caucho	1	Rotación chapa	3	0,15	3	0,3	1	0,2	1	0,05	2	0,30	1	0,45	1,45	6,46%
3.3	Chapa leva de accionamiento	1	Accionamiento microrruptor	1	0,05	3	0,3	2	0,4	2	0,10	2	0,30	1	0,45	1,60	7,13%
4	**GRUPO PLC**	1	SCHNEIDER o similar	3	0,15	3	0,3	1	0,2	2	0,10	1	0,15	2	0,90	1,80	8,02%
5	**CHAPA CENTRAL**	1	-														
5.1	Chapa central	1	Soporte y centrado del microrruptor	2	0,10	3	0,3	1	0,2	2	0,10	1	0,15	1	0,45	1,30	5,79%
5.2	Tope de caucho	2	Tope movim. carros izq. y der.	3	0,15	3	0,3	1	0,2	2	0,10	2	0,30	1	0,45	1,50	6,68%
5.3	Microrruptor	4	Sensor contacto cierre y apertura puertas	1	0,05	3	0,3	1	0,2	1	0,05	1	0,15	2	0,90	1,65	7,35%
5.4	Enclavamiento mecánico	2	Enclavam. Cierre puertas por movim. Gatillo	1	0,05	3	0,3	1	0,2	1	0,05	1	0,15	2	0,90	1,65	7,35%
																22,45	100,00%

Tabla 9.35: Características componentes significativos

9.2.11 Etapa 10: Comparación de valores finales de RAM con objetivos

Los objetivos de Fiabilidad, Mantenibilidad y Disponibilidad se comparan con los resultados obtenidos en las etapas anteriores.

- **Valores finales de RAM**

Nº.	DESCRIPCIÓN SISTEMA	Ud.	FUNCIÓN	TIPOS FALLOS	SUBSISTEMA CAUSANTE	TIPO DE INDISPONIBILIDAD
1	Unidad de control de puertas.	2	Ubicada en el andén. Controla el sistema tren-andén.	> 2 min	Fallo comunicac., acondic. señales analóg. y digit., CPU.	Averías por defectos de montaje y mal mantenimiento.
2	Módulo control.	1	Controla la puerta corredera.	Entre 15 min y 2 h	Mecanismos puertas que provocan su descarrilamiento.	Averías por defectos de montaje y mal mantenimiento.
3	Control señales sistema.	1	Grupo electrónico control motor puerta corredera.	> 2 min	Fallos circuito control potencia y comunic. PLC.	Averías por defectos de montaje y mal mantenimiento.
4	Motor.	2	Generación del movimiento y de la potencia a la correa.	> 2 min	Corrientes parásitas en bobinado por sobrecargas.	Averías por defectos de montaje y mal mantenimiento.
5	Transmisor señales tren-andén.	1	Intercambia información entre la cabecera del tren y el andén.	> 2 min	Cableado deteriorado y mal estado comunicación.	Averías por defectos de montaje y mal mantenimiento.

Tabla 9.36: Valores finales de RAM

Nº.	OBJETIVO MANTENIBILIDAD					
	MANTENIMIENTO PREVENTIVO			MANTENIMIENTO CORRECTIVO		
	Disponibilidad (A) (Objetivo ≥ 99,99%)	Fiabilidad (Objetivo ≥ 0,99992)	λ Fallos/hora (Objetivo ≤ 8·10 E-5)	TCIR tiempo por paro instalación por manten. correctivo (h)	μ (reparac./h)	MTTR (min) (Objetivo ≤ 15 min)
1	0,99999933	0,9999900	1,0E-05	0,084	15	4
2	0,99999988	0,9999982	1,8E-06	0,160	15	4
3	0,99999911	0,9999867	1,3E-05	0,080	15	4
4	0,99999990	0,9999990	1,0E-06	0,120	10	6
5	0,99999983	0,9999980	2,0E-06	0,080	12	5

Tabla 9.37: Valores finales de RAM (cont.)

Nº.	OBJETIVO DISPONIBILIDAD			
	HORAS MODO PROGRAMADO	HORAS MODO INDISPONIBILIDAD	FALLO CON INDISPONIBILIDAD MODO SERVICIO	Disponibilidad = μ/(μ+λ) (Objetivo ≥ 99,99%)
1	100.000	0,084	0,09	0,999999333
2	374.000	0,160	0,17	0,999999880
3	78.880	0,080	0,09	0,999999113
4	1.000.000	0,120	0,13	0,999999900
5	90.090	0,080	0,09	0,999999833

Tabla 9.38: Valores finales de RAM (cont.2)

- **Comparación de valores finales y objetivos de RAM**

	FIABILIDAD BÁSICA - MTBF (Tiempo medio entre fallos). Fallos que requieren una acción correctora de mantenimiento o la intervención del personal de explotación.											
Pos.	**Fallo (retraso > 2')**	**λ Fallos/h · 10E6**	**MTTR (min)**	**MTBF (horas) calculado**	**MTBF (horas) especif**	**Años/repar. Correctivo**	**Frecuencia en 32 años**	**Frec · MTTR**	**MTTR (min)**	**MTTR (min) especif**	**Disp.**	**A especif**
1	Una puerta no cierra de forma automática.	5	8	200.000	***V***	29	0,90	7,20	8	***V***	0,999960	***V***
2	Una puerta no abre de forma automática.	6	4	166.667	***V***	24	0,75	3,00	4	***V***	0,999976	***V***
3	Falla el bus de comunicaciones.	4,5	5	222.222	***V***	32	1,00	5,00	5	***V***	0,999978	***V***
4	Falla una línea de alimentación eléctrica.	8	6	125.000	***V***	18	0,56	3,38	6	***V***	0,999952	***V***
		Suma λ · 10E6		**MTBF (horas) calculado**			**Suma Frec.**	**Suma Frec*MTTR**	**Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)**		**A = Disponibilidad**	
		23,5	*<= (V)*	42.553	**14.500**		3,21	18,58	6	**15**	0,999966	**0,9999**

	FIABILIDAD SERVICIO NO VITAL - MTBF (Tiempo medio de buen funcionamiento). Fallos que obligan a intervenir al personal de mto, sin afectar al servicio ni a su seguridad.											
Pos.	**Fallo (retraso > 2')**	**λ Fallos/h · 10E6**	**MTTR (min)**	**MTBF (horas) calculado**	**MTBF (horas) especif**	**Años/repar. Correctivo**	**Frecuencia en 32 años**	**Frec · MTTR**	**MTTR (min)**	**MTTR (min) especif**	**Disp.**	**A especif**
1	Módulo de control de la puerta fuera de servicio.	1,8	5	555.556	***V***	80	0,03	0,14	5	***V***	0,999991	***V***
2	Fallo del sistema de señalización óptico.	0,05	5	20.000.000	***V***	2884	1,00	5,00	5	***V***	1,000000	***V***
3	Fallo del sistema de señalización acústico.	0,06	3	16.666.667	***V***	2403	0,83	2,50	3	***V***	1,000000	***V***
4	UCP fuera de servicio.	5	4	200.000	***X***	29	0,01	0,04	4	***V***	0,999980	***V***
		Suma λ · 10E6		**MTBF (horas) calculado**			**Suma Frec.**	**Suma Frec*MTTR**	**Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)**		**A = Disponibilidad**	
		6,91	*<= (V)*	144.718	**500.000**		1,87	7,68	4	**30**	0,999993	**0,9999**

	FIABILIDAD SERVICIO VITAL - MTBSF (Tiempo medio entre fallos que afecten al servicio). Fallos que provocan un retraso en el servicio típicamente entre 2 y 15 minutos.											
Pos.	**Fallo (retraso > 2')**	**λ Fallos/h · 10E6**	**MTTR (min)**	**MTBF (horas) calculado**	**MTBF (horas) especif**	**Años/repar. Correctivo**	**Frecuencia en 32 años**	**Frec · MTTR**	**MTTR (min)**	**MTTR (min) especif**	**Disp.**	**A especif**
1	Fallo alimentación eléctrica tiempo > 15 min.	2,6	10	384.615	***V***	55	0,58	5,77	10	***V***	0,999974	***V***
2	Módulo accionamiento puerta fuera.	1,5	8	666.667	***V***	96	1,00	8,00	8	***V***	0,999988	***V***
3	UCP fuera de servicio.	15	6	66.667	***V***	10	0,10	0,60	6	***V***	0,999910	***V***
4	Atrapamiento de ropa del usuario.	1,5	10	666.667	***V***	96	1,00	10,00	10	***V***	0,999985	***V***
		Suma λ · 10E6		**MTBF (horas) calculado**			**Suma Frec.**	**Suma Frec*MTTR**	**Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)**		**A = Disponibilidad**	
		20,6	*<= (V)*	48.544	**20.000**		2,68	24,37	9	**30**	0,999964	**0,9999**

Tabla 9.39: Comparación valores finales y objetivos de RAM

Si algún objetivo no se cumple, es necesario repetir el análisis, a no ser que se tome la decisión de disminuir las exigencias especificadas para el sistema.

10. RESULTADOS DE UN ANÁLISIS RAMS

El análisis RAM trabaja como un simulador *"what if…"* (*"que pasa si…"*), que permite inferir el impacto de nuevas políticas de mantenimiento, aplicación de nuevas tecnologías, cambios en la mantenibilidad de los equipos, modificaciones en la configuración de los procesos de producción, cambios en la política de inventarios e implantación de nuevos métodos de producción; en la disponibilidad y la producción diferida(1) del sistema.

Los principales resultados de un análisis RAMS son los siguientes:

- Pronóstico de la disponibilidad para un período determinado del sistema y de los componentes más significativos.
- Pronóstico de la fiabilidad para un período determinado del sistema y de los componentes más significativos.
- Tiempo medio de reparación de los componentes más significativos.
- Comprobación de la consecución de los objetivos de fiabilidad, disponibilidad y mantenibilidad.
- Base de Datos con información técnica, operacional y de fiabilidad del sistema.

Otros productos que resultan de un análisis RAMS son:

- Modos de fallo, causas y efectos de los distintos componentes.
- Lista jerarquizada de los equipos y sistemas críticos, con base a su impacto al factor de disponibilidad.
- Recomendaciones sobre el mantenimiento preventivo.
- Recomendaciones sobre mejoras en el diseño.
- Medidas correctiva y preventivas para reducir posibles situaciones peligrosas.

(1) Producción diferida: valor de producción programada que no se pudo completar debido a factores externos. La producción diferida de mantenimiento es el valor de producción programada que no se pudo completar debido a problemas de mantenimiento de equipos y/o sistemas.

11. CONCLUSIONES

Debido a la falta de una norma específica sobre análisis RAMS en la mayoría de sectores (existe una norma para aplicaciones eléctricas y electrónicas para ferrocarriles, UNE-EN 50126-1:2005) y, por lo tanto, a la falta de una estandarización de este análisis, este proyecto será de gran utilidad para futuros proyectos en los que se requiera el análisis RAMS, ya que se podrá utilizar la plantilla realizada con *Microsoft Office Excel 2007*.

Como se ha dicho con anterioridad, el analista debe decidir qué información es importante para su caso en concreto, por lo que deberá modificar la plantilla según sus necesidades.

La fiabilidad de los resultados obtenidos del análisis RAMS depende especialmente de la asignación de las tasas de fallo y reparación de los componentes o equipos que conforman el sistema, por lo que se ha de tener especial cuidado a la hora de obtener estos datos, ya sea a través de data histórica propia o de bases de datos externas o por la opinión de expertos.

Es conveniente realizar un análisis económico junto al análisis RAMS, ya que las acciones de mitigación y mejora deben estar basadas en un análisis costo-riesgo.

El análisis RAMS se ha de ir actualizando a lo largo del ciclo de vida del sistema, ya que es muy útil en las distintas fases, diseño, fabricación, instalación, operación y mantenimiento y mejoras.

Los resultados mostrados en el *apartado 10* demuestran la gran utilidad de este análisis, debido a que la comprobación de los objetivos de fiabilidad, disponibilidad, mantenibilidad y seguridad debe ser una actividad fundamental de cualquier proyecto.

12. BIBLIOGRAFÍA

[1] Amendola, Luis. Indicadores de fiabilidad propulsores en la gestión del mantenimiento. Universidad Politécnica de Valencia.

[2] Arques Patón, José Luis (2009). *Ingeniería y gestión del mantenimiento en el sector ferroviario*.

[3] Arriba Arroyo, Raquel (2009). *Estudio del coste de vida de un sistema de señalización ferroviario*. Proyecto Fin de Carrera. Universidad Carlos III de Madrid.

[4] Creus Sole, Antonio (2005). *Fiabilidad y Seguridad*.

[5] García de Korazar, Xabier (2004). Proceso de mejora de RAMS a lo largo del ciclo de vida (I). *IMHE: Información de máquinas-herramienta, equipo y accesorios*, 304, 103-110.

[6] García de Korazar, Xabier (2004). Proceso de mejora de RAMS a lo largo del ciclo de vida (II). *IMHE: Información de máquinas-herramienta, equipo y accesorios*, 305, 60-65.

[7] Gómez de la Vega H., Medina N., Semeco K, Yanez M. *Análisis de Confiabilidad, Disponibilidad y Mantenibilidad en Sistemas Productivos*. Reliability and Risk Management S.A.

[8] Grupo universitario de investigación analítica de riesgos (2011, Marzo). Disponible en: http://www.unizar.es/guiar

[9] Madrigal Landeros, E. 2004. *Estimación e inferencia de los parámetros de la distribución Hockey Stick*. Tesis Maestría. Universidad de las Américas Puebla.

[10] Mantenimiento mundial (2011, Febrero). Disponible en: http://www.mantenimientomundial.com

[11] Marco Pascual, Pol (2010). *Estudio de optimización de un sistema de tracción eléctrica*. Universitat Politècnica de Catalunya.

[12] Métodos comparativos de análisis de riesgo (2012, Enero). Disponible en: http://www.unizar.es/guiar/1/Accident/An_riesgo/Met_comp.htm#PHA

[13] Plazas Aguilar, Jaime (2010). *Ingeniería de confiabilidad aplicada a un sistema de control local en una planta de transporte de hidrocarburos*. Proyecto Fin de Carrera. Universidad de los Andes.

[14] Reliability & Risk Management (2011, Febrero). Disponible en: http://www.reliarisk.com

[15] UNE-EN 60812 Técnicas de análisis de la fiabilidad de sistemas. Procedimiento de análisis de los modos de fallo y de sus efectos (AMFE), Diciembre 2008.

[16] UNE-EN 61025 Análisis por árbol de fallos (AAF), Enero 2011.

[17] UNE-EN 61078 Técnicas de análisis de la confiabilidad. Método del diagrama de bloques de la fiabilidad y métodos booleanos, Diciembre 2006.

ANEXOS

PLANTILLA EN EXCEL:

	PLAN RAM							
	FIABILIDAD BÁSICA - MTBF (Tiempo medio entre fallos). Fallos que requieren una acción correctora de mantenimiento o la intervención del personal de explotación para restablecer la funcionalidad del sistema.				Gravedad de los Fallos			
Pos.	Fallo	Fallos/h · 10E6	MTTR (min)	Efectos	I Catastr.	II Crítico	III Marginal	IV Insignific.
1								
2								
3								
4								
	FIABILIDAD SERVICIO NO VITAL - MTBF (Tiempo medio de buen funcionamiento). Fallos que obligan a intervenir al personal de mantenimiento, sin afectar al servicio.				Gravedad de los Fallos			
Pos.	Fallo	Fallos/h · 10E6	MTTR (min)	Efectos	I Catastr.	II Crítico	III Marginal	IV Insignific.
1								
2								
3								
4								
	FIABILIDAD SERVICIO VITAL - MTBSF (Tiempo medio entre fallos que afecten al servicio). Fallos que provocan un retraso en el servicio.				Gravedad de los Fallos			
Pos.	Fallo	Fallos/h · 10E6	MTTR (min)	Efectos	I Catastr.	II Crítico	III Marginal	IV Insignific.
1								
2								
3								
4								

ANÁLISIS PREVIO FMECA

Nº.	Descripción	Ud.	Función	Modos de fallo		Causas de fallo	Consecuencias del fallo		Detección del fallo	Dispositivos alternativos	Probabilidad de fallo					Nivel de criticidad			
				Generales	Genéricos		Efecto local	Efecto final			Muy baja	Baja	Media	Alta	Muy Alta	I	II	III	IV

ANÁLISIS PRELIMINAR DE DISPONIBILIDAD

Nº.	Descripción	Ud.	Función	λ (Fallos/h) · 10E6	μ - Nº Operaciones mantenimiento/h	D(∞) =1/(1+λ/μ)

ANÁLISIS POR ÁRBOL DE FALLOS

Descripción Fallos	λ (Fallo/año)	λ (Fallo/hora)· 10E6	Infiabilidad exponencial (en un año) (1-exp(-λt))	Fiabilidad exponencial (en un año) (exp(-λ·t))

DIAGRAMA DE BLOQUES DE FIABILIDAD			
Descripción Fallos	λ (Fallo/año)	λ (Fallo/hora)	Fiabilidad exponencial/hora (exp(-λ·t))

MANTENIMIENTO PREVENTIVO											
OPERACIONES POR REALIZAR	PERIODICIDAD		TIEMPOS DE INTERVENCIÓN (minutos)	Nº. OPERARIOS MANTENIMIENTO	CALIDAD DEL SERVICIO (QoS)		DISPONIBILIDAD DE SERVICIO (Objetivo: _%) D = MTBF/(MTBF + MTTR)	FIABILIDAD SISTEMA (Objetivo: _%)			RECOMENDACIONES
	CICLOS	MESES			MTBF (horas)	MTTR (minutos)		λ fallos/h · 10E6	Redundancía (Sí/No)	Fiabilidad	

REPARACIÓN								
Ítem	DESCRIPCIÓN	CANTIDAD	FUNCIÓN	MTTR (minutos)	PROBABILIDAD FALLO - λ (fallos/h)·10E6	MTTR (minutos)		
						T. DIAGNÓSTICO	T. RECAMBIO Y AJUSTE	T. PUESTA EN SERVICIO

DISPONIBILIDAD, HIPÓTESIS, CONCLUSIONES Y PROPUESTAS

Ítem	DESCRIPCIÓN	CANTIDAD	FUNCIÓN	MTBF (horas)	MTBSF - DISPONIBILIDAD DE SERVICIO	HIPÓTESIS DE PARTIDA Y BASES DE DATOS DE CÁLCULO	DISEÑO				PROPUESTA DE COMPROBACIÓN, VERIFICACIÓN EMPÍRICA Y CERTIFICACIÓN DE LOS VALORES OFERTADOS	
							CONCLU-SIONES	RECOMEN-DACIONES	ACCIONES CORRECTORAS	REDUN-DANCIAS	PROTOTIPOS	INSTALACIÓN TERMINADA PENDIENTE DEL PERÍODO DE GARANTÍA

ANÁLISIS DE RIESGOS

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	MODO DE FALLO (Cómo se detecta)	EFECTOS DEL FALLOS (Operación, Función o	DETECCIÓN FALLO Y MÉTODOS PROTECCIÓN	Índice Severidad (S) (1 a 5) o (1 a 10)	Índice Ocurrencia (O) (1 a 5) o (1 a 10)	Índice Detección (D) (1 a 5) o (1 a 10)	Índice Criticidad (RPN = S·O·D)

ANÁLISIS DE RIESGOS

Nº.	SIL (Safety Integrity Level)	PROBABILIDAD FALLOS A LA DEMANDA (PFD)	DISPONIBILIDAD (1 - PFD)	(1/PFD)	RIESGO EN SEGURIDAD PERSONAS	MEDIDAS CORRECTIVAS O PREVENTIVAS PARA REDUCIR EL PELIGRO

ESTUDIO PREVIO RAMS

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	MODO DE FALLO (Cómo se detecta)	DETECCIÓN FALLO Y MÉTODOS PROTECCIÓN	EFECTOS DEL FALLOS (Operación, Función o Estado del sistema)	Índice Severidad (S) (1 a 5) o (1 a 10)	Índice Ocurrencia (O) (1 a 5) o (1 a 10)	Índice Detección (D) (1 a 5) o (1 a 10)	Índice Criticidad (RPN = S·O·D)

ESTUDIO PREVIO RAMS

Nº.	SIL (Safety Integrity Level)	λ (Fallo/h)·10E6	λ (Fallo/año)	FIABILIDAD (1-λ)	MTBF (1/λ)	MTTR (min)	μ (Nº reparac./h) = 1/MTTR	DISPONIBILIDAD μ/(μ+λ)	SOFTWARE λ	FIABILIDAD DEL SOFTWARE

ESTUDIO PREVIO RAMS

Nº.	MANTENIMIETO PREVENTIVO					MANTENIMIENTO CORRECTIVO						PLANES CONTINGENCIA	AISLAMIENTO, FALLOS Y AVERÍAS
	Periodicidad (horas)	Tiempo respuesta (horas)	Personal	Material	Coste material	λ (Fallo/hora) ·10E6	MTBF (horas)	Tiempo respuesta (horas)	Personal	Material	Coste material		

CARACTERÍSTICAS COMPONENTES

Nº.	DESCRIPCIÓN	Ud.	FUNCIÓN	FACTORES DE CONTRIBUCIÓN A LA DISPONIBILIDAD DEL SISTEMA												CONTRIBUCIÓN DE CADA ELEMENTO	
				COMPLEJIDAD		ESTADO		TIEMPO DE FUNCIONAMIENTO		CONDICIONES DE CONTORNO		FACILIDAD DE REPARACIÓN		REDUNDANCIA		Peso	Ponderación sobre el total

VALORES FINALES DE RAM						
Nº.	DESCRIPCIÓN SISTEMA	Ud.	FUNCIÓN	TIPOS FALLOS	CAUSA	TIPO DE INDISPONIBILIDAD

VALORES FINALES DE RAM						
Nº.	OBJETIVO MANTENIBILIDAD					
	MANTENIMIENTO PREVENTIVO			MANTENIMIENTO CORRECTIVO		
	Disponibilidad (A) (Objetivo ≥ _%)	Fiabilidad (Objetivo ≥ __)	λ Fallos/hora (Objetivo ≤ __)	TCIR tiempo por paro instalación por manten. correctivo (h)	μ (Nº reparac./h)	MTTR (min) (Objetivo ≤ 15 min)

VALORES FINALES DE RAM				
Nº.	OBJETIVO DISPONIBILIDAD			
	HORAS MODO PROGRAMADO	HORAS MODO INDISPONIBILIDAD	FALLO CON INDISPONIBILIDAD MODO SERVICIO	Disponibilidad = μ/(μ+λ) (Objetivo ≥ 99,99%)

COMPROBACIÓN DE OBJETIVOS

FIABILIDAD BÁSICA - MTBF (Tiempo medio entre fallos).
Fallos que requieren una acción correctora de mantenimiento o la intervención del personal de explotación.

Pos.	Fallo	λ Fallos/h · 10E6	MTTR (min)	MTBF (horas) calculado	MTBF (horas) especificado	Años/repar. Correctivo	Frecuencia en X años	Frec · MTTR	MTTR (min)	MTTR (min) especificado	Disponibilidad	A = Disponibilidad especificada
1												
2												
3												
4												
		Suma λ · 10E6		MTBF (horas) calculado			Suma Frec.	Suma Frec*MTTR	Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)		A = Disponibilidad	

FIABILIDAD SERVICIO NO VITAL - MTBF (Tiempo medio de buen funcionamiento).
Fallos que obligan a intervenir al personal de mto, sin afectar al servicio ni a su seguridad.

Pos.	Fallo	λ Fallos/h · 10E-6	MTTR (min)	MTBF (horas) calculado	MTBF (horas) especificado	Años/repar. Correctivo	Frecuencia en X años	Frec · MTTR	MTTR (min)	MTTR (min) especificado	Disponibilidad	A = Disponibilidad especificada
1												
2												
3												
4												
		Suma λ · 10E6		MTBF (horas) calculado			Suma Frec.	Suma Frec*MTTR	Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)		A = Disponibilidad	

FIABILIDAD SERVICIO VITAL - MTBSF (Tiempo medio entre fallos que afecten al servicio).
Fallos que provocan un retraso en el servicio típicamente entre 2 y 15 minutos.

Pos.	Fallo	λ Fallos/h · 10E-6	MTTR (min)	MTBF (horas) calculado	MTBF (horas) especificado	Años/repar. Correctivo	Frecuencia en X años	Frec · MTTR	MTTR (min)	MTTR (min) especificado	Disponibilidad	A = Disponibilidad especificada
1												
2												
3												
4												
		Suma λ · 10E6		MTBF (horas) calculado			Suma Frec.	Suma Frec*MTTR	Tiempo medio invertido (min) = (Suma Frec*MTTR)/ (Suma Frec)		A = Disponibilidad	